UNIVERSIDAD DE MURCIA

http://revistas.um.es/analesderecho

ANALES de DERECHO

# LA POTESTAD SANCIONADORA DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EN MATERIA DE TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL

ALFONSO ORTEGA GIMÉNEZ

Profesor Titular de Derecho Internacional Privado

Universidad Miguel Hernández de Elche

***La potestad sancionadora de la Agencia Española de Protección de Datos en materia de transferencias internacionales de datos de carácter personal****

***Resumen***

*El diseño de una normativa reguladora adecuada, efectiva y eficaz que tienda a la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos constituye un auténtico desafío. Se trata de una materia no exenta del poder sancionador de la AEPD. En los últimos años (2010-2024) ha llegado a abrir 15 procedimientos sancionadores a Administraciones Públicas y/o a diferentes entidades interponiendo cuantiosas sanciones por infracción del régimen jurídico previsto (en el RGPD y en la LOPDGDD) en materia de transferencias internacionales de datos. El objeto del presente trabajo es: realizar un análisis práctico de las sanciones impuestas por la AEPD en materia de transferencias internacionales de datos, en el periodo 2010-2024.*

***Palabras clave:*** *protección de datos, procedimiento sancionador, AEPD, transferencia internacional de datos.*

***The sanctioning power of the Spanish Data Protection Agency in matters of international transfers of personal data***

***Abstract***

*The design of an adequate, effective and efficient regulatory regulation aimed at protecting the holder of the right to data protection derived from an international transfer of data constitutes a real challenge. This is a matter that is not exempt from the sanctioning power of the AEPD. In recent years (2010-2024) it has opened 15 sanctioning proceedings against Public Administrations and/or different entities, imposing heavy penalties for infringement of the legal regime provided for (in the RGPD and in the LOPDGDD) in matters of international data transfers. The purpose of this paper is: to carry out a practical analysis of the sanctions imposed by the AEPD on international data transfers in the period 2010-2022.*

***Keywords****: data protection, sanctioning procedure, AEPD, international data transfer****.***

* Este trabajo se enmarca en el proyecto "La potestad sancionadora de las autoridades de control en materia de protección de datos: delimitación, garantías y efectos" (ref. PID2022-139265OB-I00), investigadores principales: Julián Valero Torrijos y María Magnolia Pardo López. El proyecto está financiado por Gobierno de España a través del Ministerio de Ciencia e Innovación -Agencia Estatal de Investigación en la convocatoria «Proyectos de Generación de Conocimiento» y a actuaciones para la formación de personal investigador predoctoral asociadas a dichos proyectos, del Programa Estatal para Impulsar la Investigación Científico-Técnica y su Transferencia, en el marco del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023. Período de ejecución: 2023-2025. El proyecto corresponde a la convocatoria 2022 de «Proyectos de Generación de Conocimiento» y actuaciones para la formación de personal investigador predoctoral asociadas a dichos proyectos, en el marco del Programa Estatal para Impulsar la Investigación Científico-Técnica y su Transferencia, del Plan Estatal de Investigación Científica, Técnica y de Innovación 2021-2023. Cuantía: 47.500 (total) 38.000 (costes directos) 9.500 (costes indirectos).

**SUMARIO**: I. PLANTEAMIENTO. - II. BREVE APROXIMACIÓN A LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL RGPD Y EN LA LOPDGDD. - III. PROCEDIMIENTOS SANCIONADORES ABIERTOS POR LA AEPD EN EL PERIODO 2010-2024. ANÁLISIS PRÁCTICO DE ALGUNOS PROCEDIMIENTOS SANCIONADORES EN MATERIA DE TRANSFERENCIAS INTERNACIONALES DE DATOS. - IV. REFLEXIÓN FINAL.

## I. PLANTEAMIENTO

Las transferencias internacionales de datos no son una materia exenta del poder sancionador de la Agencia Española de Protección de Datos (en adelante, AEPD). En los últimos años (2010-2024), la AEPD ha llegado a abrir 15 procedimientos sancionadores a Administraciones Públicas y/o a diferentes entidades (Asociaciones, Fundaciones, empresas de telecomunicaciones, del sector bancario y del sanitario) interponiendo cuantiosas sanciones por infracción del régimen jurídico previsto en el RGPD y en la LOPDGDD en materia de transferencias internacionales de datos. El objeto del presente trabajo es, tras una breve aproximación normativa a las transferencias internacionales de datos en el RGPD y en la LOPDGDD, realizar un análisis práctico de las sanciones impuestas por la AEPD en materia de transferencias internacionales de datos en el periodo 2010-2024[1].

El diseño de una normativa reguladora adecuada, efectiva y eficaz que tienda a la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal constituyen un auténtico desafío. Y ello por varios motivos: a) en primer lugar, por la creciente dimensión económica que está cobrando el libre tránsito de la información. El acceso y uso de la información por parte de empresas, administraciones e individuos se ha convertido en un precioso bien intangible, causa y efecto a la vez de la progresiva integración económica y social; b) en segundo lugar, porque junto a la dimensión económica, la protección de los datos personales y de la intimidad supone afrontar por vez primera la difícil tarea de compatibilizar los derechos fundamentales con el comercio internacional. Y todo ello en cada una de las distintas esferas jurídicas implicadas; y,

[1] *Vid.* https://www.aepd.es/informes-y-resoluciones/resoluciones?fecha_firma_desde=2010&fecha_firma_hasta=2024&search_api_fulltext=&f%5B0%5D=conceptos%3A1555&sort_bef_combine=fecha_firma_ASC [Fecha de consulta: 26/09/2024].

c) en tercer lugar, porque la especial volatilidad de las transferencias internacionales de datos complica extraordinariamente la definición del derecho sustantivo aplicable. En este contexto, emerge el Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 25 de enero de 2012 (en adelante, Reglamento General de Protección de Datos o RGPD) [2], norma general y directamente aplicable sin necesidad de transposición; el objetivo es claro: lograr la uniformidad legislativa[3], simplificando el régimen jurídico en materia de transferencias internacionales de datos[4]; y, un tiempo después, la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD)[5].

## II. BREVE APROXIMACIÓN A LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL RGPD Y EN LA LOPDGDD

Una vez adoptada la decisión por parte de la Comisión Europea, se prevé la posibilidad de transmitir datos personales a terceros Estados con un nivel de protección adecuado, siendo éste un elemento clave para considerar válidas las transferencias internacionales.

El artículo 45 fija los criterios, condiciones y procedimientos para la adopción de una decisión relativa a la adecuación del nivel de protección de datos por parte de la Comisión, basada en el artículo 25 de la Directiva 95/46/CE[6].

Se confirma explícitamente la posibilidad de que la Comisión Europea evalúe el nivel de protección que ofrece un territorio o un sector de tratamiento en un tercer país. Para las transferencias a terceros países, en relación con las cuales la Comisión no haya adoptado ninguna decisión de adecuación, el artículo 46 requiere que se aporten las garantías

[2] COM (2012) 11 final.

[3] *Vid.* SOLAR CALVO, P., "La doble vía europea en protección de datos", *Diario La Ley*, N.º 7832, Sección Doctrina, Año XXXIII, Editorial LA LEY, Madrid, 4 de abril de 2012,

[4] *Vid.* DELGADO CARRAVILLA, E y PUYOL MONTERO, J., *La implantación del nuevo Reglamento de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018, pp. 323-385.

[5] BOE *núm.* 294, de 6 de diciembre de 2018.

[6] *Vid.* HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Editorial Aranzadi, Elcano (Navarra), 1997, 185-189.

apropiadas, especialmente cláusulas tipo de protección de datos, normas corporativas vinculantes y cláusulas contractuales.

La decisión de la Comisión ante la posibilidad de hacer uso de cláusulas tipo de protección de datos se basa en el artículo 26, apartado 4, de la Directiva 95/46/CE[7]. Como novedad, estas cláusulas tipo de protección de datos también pueden ser adoptadas por una autoridad de control y ser declaradas generalmente válidas por la Comisión. En la actualidad, las normas corporativas vinculantes se mencionan específicamente en el texto jurídico. La opción de las cláusulas contractuales ofrece cierta flexibilidad al responsable o al encargado del tratamiento, aunque está sujeta a la autorización previa por parte de las autoridades de control.

Una de las más destacables novedades introducidas en el RGPD la encontramos en su artículo 47, que hace referencia a las normas corporativas vinculantes, en el que se establece que "la autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia". Con lo cual, la batería de normas que se aprueben deberán ser de obligado cumplimiento, siempre y cuando cumpla con los requisitos que establece el artículo 47.1 del Reglamento, siendo éste el que otorga tal fuerza vinculante.

Así pues, se podrían definir las normas corporativas vinculantes como normas internas (como un código de conducta) adoptadas por un grupo multinacional de empresas que definen su política global, con respecto a las transferencias internacionales de datos personales, dentro de un mismo grupo empresarial, a entidades situadas en países que no ofrecen un nivel adecuado de protección. Están destinadas únicamente a los grupos empresariales.

El artículo 49 define y aclara las excepciones a una transferencia de datos sobre la base de las disposiciones en vigor del artículo 26 de la Directiva 95/46/CE. Ello se aplica, en particular, a las transferencias de datos requeridas y necesarias para la protección de intereses públicos importantes, por ejemplo, en caso de transferencias internacionales de

[7] *Vid.* HEREDERO HIGUERAS, M., *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Editorial Aranzadi, Elcano (Navarra), 1997, 190-194.

datos entre autoridades de competencia, administraciones fiscales o aduaneras, o entre servicios competentes en materia de seguridad social o de gestión de la pesca.

Antes de proseguir, resulta necesario destacar que, en determinadas circunstancias, una transferencia de datos personales puede estar justificada por un interés legítimo del responsable o del encargado del tratamiento, aunque únicamente después de haber evaluado y documentado las circunstancias de dicha operación de transferencia, es decir, a través de un *numerus clausus se* establece una serie de situaciones en las que no será necesaria una decisión de adecuación ni garantías de adecuación y sin que sea necesaria la autorización de las autoridades de control.

No obstante, es cierto que el Reglamento establece una lista cerrada de supuestos que parece limitan aquellas situaciones en que pueden concurrir, lo que no escapa de la crítica al considerar que dicha lista, ofrecida por el artículo 49, es demasiado amplia. Incluso en unos de sus apartados (art. 49.1.g)) establece que puede realizarse una transferencia de datos personales *aún cuando no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado*[8].

Por su parte, la LOPDGDD (artículo 40 –"Régimen de las transferencias internacionales de datos"–) consolida en materia de transferencias internacionales de datos de carácter personal un marco jurídico (representado por el RGPD) moderno, sólido, coherente y global de protección de datos para la UE y para terceros Estados. Un marco legislativo sólido y coherente, que potencia la dimensión de mercado único de la protección de datos (= desaparición de los diferentes niveles de protección en cada uno de los Estados miembros de la UE, consecuencia de la disparidad existente entre sus disposiciones legales, reglamentarias, y administrativas) con el fin último de favorecer las relaciones comerciales entre la UE y terceros Estados.

El artículo 41 de la LOPDGDD ("Supuestos de adopción por la Agencia Española de Protección de Datos") vaticina que la AEPD y las autoridades autonómicas de protección de datos podrán adoptar cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos.

[8] Considerandos 111 a 113 del RGPD.

La AEPD y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del RGPD ("Normas corporativas vinculantes"). El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del RGPD ("Dictamen del Comité"), y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

De acuerdo con lo previsto en el artículo 42 de la LOPDGDD ("Supuestos sometidos a autorización previa de las autoridades de protección de datos"), las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo 41 de la LOPDGDD ("Supuestos de adopción por la Agencia Española de Protección de Datos") y en el artículo 46.2 del RGPD ("Transferencias mediante garantías adecuadas"), requerirán una previa autorización de la AEPD o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos: a) cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo; o, b) cuando la transferencia se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

La autorización quedará sometida a la emisión del dictamen por el Comité Europeo de Protección de Datos (artículos 64.1.e), 64.1.f) y 65.1.c) del RGPD –"Dictamen del Comité y Resolución de conflictos por el Comité" –). La remisión del expediente al citado Comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la AEPD o, por conducto de esta, a la autoridad de control competente, en su caso.

Conforme a lo previsto en el artículo 43 de la LOPDGDD ("Supuestos sometidos a información previa a la autoridad de protección de datos competente"), los responsables del tratamiento deberán informar a la AEPD o, en su caso, a las autoridades autonómicas de protección de datos, cuando se trate de una transferencia internacional de datos sobre

la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por el responsable y no prevalezcan los derechos o intereses del interesado, siempre que concurran también los requisitos siguientes (último párrafo del artículo 49.1 del RGPD –"Excepciones para situaciones específicas" –): a) no sea repetitiva; b) afecte sólo a un número limitado de interesados; y, c) el responsable haya evaluado todas las circunstancias concurrentes. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos; información que deberá facilitarse con carácter previo a la realización de la transferencia. No obstante, esta exigencia de información previa no se aplicará a las actividades llevadas a cabo por las autoridades en el ejercicio de sus poderes públicos (artículo 49.3 del RGPD –"Excepciones para situaciones específicas" –).

Las autoridades autonómicas de protección de datos, tal y como prevé el artículo 61 de la LOPDGDD ("Intervención en caso de tratamientos transfronterizos"), ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del RGPD ("Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas") cuando se refiera a un tratamiento previsto en el artículo 57 de la propia LOPDGDD ("Autoridades autonómicas de protección de datos"), que se llevará a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del RGPD ("Competencia de la autoridad de control principal"), salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

En estos casos corresponderá a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del RGPD ("Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas"), informando a la AEPD sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

## III. PROCEDIMIENTOS SANCIONADORES ABIERTOS POR LA AEPD EN EL PERIODO 2010-2024. ANÁLISIS PRÁCTICO DE ALGUNOS PROCEDIMIENTOS SANCIONADORES EN MATERIA DE TRANSFERENCIAS INTERNACIONALES DE DATOS

Si queremos dar una respuesta efectiva a los nuevos retos que plantea la garantía efectiva del derecho fundamental a la protección de datos; y, en particular, en su dimensión trasnacional, se deben establecer mecanismos reales de vigilancia y control que superen las barreras nacionales. Y deben ser las Autoridades de protección, de cada Estado miembro, quienes tomen parte en las tareas de investigación, coordinación y cooperación con otras autoridades de protección de otros Estados.

Bajo el paraguas/contexto del endurecimiento y agravamiento del régimen sancionador en el RGPD, la AEPD, como el resto de las demás autoridades de protección de los Estados miembros de la UE tienen que garantizar que la imposición de multas administrativas se produzca, en cada caso, de manera individual, de forma efectiva y con carácter proporcionado y disuasorio ante la infracción cometida. No obstante, la imposición de multas administrativas se ha atemperado en el caso de los procedimientos sancionadores en materia de transferencias internacionales de datos, y en aras a la gravedad y a la cuantía de las sanciones económicas, y las muchas circunstancias que es necesario ponderar a los efectos de la imposición de estas multas administrativas en materia de transferencias internacionales de datos; lo que en la práctica le ha permitido a la AEPD, bajo los criterios de proporcionalidad y de efectividad, sustituirlas por otras medidas tales como la suspensión de los flujos de datos hacia el exterior[9].

En el periodo 2010-2024 podemos identificar los siguientes procedimientos sancionadores abiertos por la AEPD:

A las ADMINISTRACIONES PÚBLICAS:

a) Procedimiento de Declaración de Infracción de Administraciones Públicas AP/00024/2018, de fecha 27 de diciembre de 2018[10].

A INSTITUCIONES:

[9] *Vid.* DELGADO CARRAVILLA, E y PUYOL MONTERO, J., *La implantación del nuevo Reglamento de Protección de Datos de la Unión Europea*, Tirant lo Blanch, Valencia, 2018, pp. 84-90.

[10] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/aapp-00024-2018.pdf [Fecha de consulta: 26/09/2024].

a) Resolución de archivo de las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad UNIVERSIDAD COMPLUTENSE DE MADRID, de fecha 17 de julio de 2018[11].

A EMPRESAS Y ENTIDADES:

a) Resolución de caducidad de actuaciones ante la autoridad de protección de datos de Países Bajos contra BANKINTER, S.A., de fecha 25 de abril de 2022[12].

b) Procedimiento sancionador PS/00137/2018, instruido por la Agencia Española de Protección de Datos a la entidad SEGUR IBÉRICA, S.A., de fecha 26 de diciembre de 2018[13].

c) Procedimiento sancionador a las entidades GOOGLE SPAIN, S.L. y GOOGLE INC., de fecha 3 de octubre de 2017[14].

d) Procedimiento sancionador PS/00541/2010 a las entidades GOOGLE Inc. (actualmente GOOGLE LLC) y GOOGLE SPAIN, S.L, de fecha 20 de octubre de 2017[15].[16]

e) Procedimiento sancionador PS/00391/2016, a la entidad ASSEMBLEA NACIONAL CATALANA, OMNIUM CULTURAL, de fecha 4 de mayo de 2017[17].

[11] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-06555-2017.pdf [Fecha de consulta: 26/09/2024].

[12] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-02670-2020.pdf [Fecha de consulta: 26/09/2024].

[13] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/ps-00137-2018.pdf [Fecha de consulta: 26/09/2024].

[14] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/reposicion-ps-00541-2010.pdf [Fecha de consulta: 26/09/2024].

[15] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/ps-00541-2010.pdf [Fecha de consulta: 26/09/2024].

[16] Este procedimiento sancionador fue instruido por las actuaciones practicadas por la Agencia Española de Protección de Datos a las entidades GOOGLE Inc. (actualmente GOOGLE LLC) y GOOGLE SPAIN, S.L., de oficio. *Vid.* https://www.aepd.es/documento/e-06190-2012.pdf [Fecha de consulta: 26/09/2024].

[17] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/ps-00391-2016.pdf [Fecha de consulta: 26/09/2024].

f) Procedimiento sancionador PS/00371/2016, a la entidad ASOCIACIÓN DE TÉCNICOS DE INFORMÁTICA, de fecha 22 de marzo de 2017[18].

g) Recurso de reposición interpuesto por la entidad ASSEMBLEA NACIONAL CATALANA contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00391/2016, de fecha 4 de mayo de 2017[19].

h) Recurso de reposición interpuesto por la entidad OMNIUM CULTURAL contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos en el procedimiento sancionador, PS/00391/2016, de fecha 22 de febrero de 2017[20].

i) Resolución de archivo de actuaciones ante la FUNDACIÓN DE INVESTIGACIÓN HM HOSPITALES, y la FUNDACIÓN JIMÉNEZ DIAZ, de fecha 30 de mayo de 2016[21].

j) Recurso de reposición interpuesto por FACUA - CONSUMIDORES EN ACCIÓN contra la resolución dictada por el Director de la Agencia Española de Protección de Datos en el expediente de actuaciones previas de inspección E/06406/2012, de fecha 5 de diciembre de 2013[22].

k) Resolución de archivo de actuaciones ante las entidades AEROVIAS DE MEXICO SA DE C.V. (AEROMEXICO), AIR EUROPA LINEAS AEREAS SA, IBERIA LINEAS AEREAS DE ESPAÑA SOCIEDAD ANONIMA

[18] *Vid*. Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/ps-00371-2016.pdf [Fecha de consulta: 26/09/2024].

[19] *Vid*. Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/reposicion-ps-00391-2016b.pdf [Fecha de consulta: 26/09/2024].

[20] *Vid*. Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/reposicion-ps-00391-2016.pdf [Fecha de consulta: 26/09/2024].

[21] *Vid*. Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-05966-2015.pdf [Fecha de consulta: 26/09/2024].

[22] *Vid*. Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/reposicion-e-06406-2012.pdf [Fecha de consulta: 26/09/2024].

OPERADORA en virtud de denuncia presentada por FACUA - CONSUMIDORES EN ACCION, de fecha 20 de septiembre de 2013[23].

l) Resolución de archivo de actuaciones ante la entidad TELEFÓNICA ESPAÑA, S.A.U., de fecha 23 de julio de 2010[24].

A continuación, nos vamos a centrar en el análisis práctico de algunos de esos procedimientos sancionadores abiertos y resueltos por la AEPD en materia de transferencias internacionales de datos relacionados con: 1) la vulneración del principio general de las transferencias internacionales de datos; 2) las transferencias internacionales de datos mediante garantías adecuadas; 3) la aplicación territorial de la normativa española en materia de protección de datos en el marco de las actividades de un establecimiento del responsable del tratamiento en territorio español o cuando se han empleado medios situados en España por parte de un responsable del tratamiento no establecido en la UE; 4) la vulneración del derecho de información y acceso a los datos personales en relación con una transferencia internacional de datos; y, 5) la caducidad de las actuaciones en el ejercicio del derecho de acceso dentro del marco de las transferencias internacionales de datos.

En particular, nos referimos a los siguientes procedimientos sancionadores:

**1)** Vulneración del principio general de las transferencias internacionales de datos (Procedimiento de Declaración de Infracción de Administraciones Públicas AP/00024/2018, de fecha 11 de enero de 2019) [25].

La declaración de infracción en el PS/0021/2017, de 7 de noviembre de 2017, acredita que el Centro los Tilos (Generalitat de Cataluña, Dirección General de ejecución penal a la comunidad y de justicia juvenil), como responsable del tratamiento, dio instrucciones al personal de vigilancia del citado Centro para crear una cuenta de correo electrónico, con la finalidad de poder comunicarse con la persona de vigilancia y seguridad. A través de la dirección electrónica, la dirección del centro los Tilos proporcionaba al personal de

[23] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-06406-2012.pdf [Fecha de consulta: 26/09/2024].

[24] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-02238-2008.pdf [Fecha de consulta: 26/09/2024].

[25] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/aapp-00024-2018.pdf [Fecha de consulta: 26/09/2024].

vigilancia y seguridad datos de los menores internos entre los que había datos de salud (no menciona cuales). Con esta situación, la dirección de los Tilos no garantizaba la seguridad de los datos ya que la transmisión se efectuaba sin cifrar los datos personales y sin utilizar otro mecanismo equivalente que garantizara que la información no fuera ininteligible ni manipulada por tercero. No menciona la cuenta de correo de que se trata, aunque se desprende que la cuenta es ***EMAIL.4@gmail.com. El 22/12/2016 se dio de baja la citada cuenta de correo electrónico.

La dirección Gmail se corresponde con la utilizada por el servidor de correo electrónico del servicio gratuito de correo electrónico prestado por la empresa estadounidense GOOGLE LLC. Según consta en información extraída de internet, dicha entidad se asoció al sistema PRIVACY SHIELD el 22/09/2016, si bien su solicitud fue realizada el 29/08/2016.

La transferencia internacional de datos producida y que se imputa tiene que ver con la puesta en el servidor del correo Gmail, titularidad de GOOGLE, de mensajes de correo electrónico enviados usando como remitente o destinatario dicha dirección, y conteniendo datos de carácter personal.

En este caso, analizando el periodo en el que se entendería cometida la infracción, consiste en envío de mensajes utilizando dirección Gmail entre cuentas de correos electrónicos, resulta necesario analizar la Sentencia del asunto Caso Schrems C 362-2014, de 6 de noviembre de 2015, del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) que anula la decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada. En el examen de la validez que hace el Tribunal de Justicia sobre la citada Decisión, el TJUE recuerda que la Comisión estaba obligada a comprobar si Estados Unidos garantiza efectivamente, debido a su legislación interna o de sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente al garantizado en la Unión en virtud de la Directiva, interpretada a la luz de la Carta. El TJUE observa que la Comisión no llevó a cabo ese examen, sino que se limitó a analizar el régimen de puerto seguro.

El TJUE señala que el nivel de protección sustancialmente equivalente al garantizado en la Unión únicamente es aplicable a las entidades estadounidenses que se han adherido a

él, de modo que las autoridades estadounidenses no están sometidas a dicho régimen. Además, las exigencias de seguridad nacional, interés público y cumplimiento de la ley de Estados Unidos prevalecen sobre el régimen de puerto seguro, de modo que las entidades estadounidenses están obligadas a dejar de aplicar, sin limitación, las reglas de protección previstas por ese régimen cuando entren en conflicto con las citadas exigencias. El régimen estadounidense de puerto seguro posibilita, de ese modo, injerencias por parte de las autoridades estadounidenses en los derechos fundamentales de las personas, y la Decisión de la Comisión no pone de manifiesto que en Estados Unidos haya reglas destinadas a limitar esas posibles injerencias ni que exista una protección jurídica eficaz contra éstas.

Hay que tener en cuenta que GOOGLE, titular de la dirección Gmail, se asocia al sistema nuevo, de *Privacy Shield*, el 22/09/2016 habiendo remitido la solicitud de adhesión el 29/08/2016 para acogerse a la decisión de ejecución 2016/1250 UE de 12/07 con arreglo a la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU.

La AEPD resolvió declarando el ARCHIVO de la infracción imputada a la DIRECCIÓN GENERAL D'EXECUCIÓ PENAL A LA COMUNIDAD Y DE JUSTICIA JUVENIL (CENTRE EDUCATIU ELS TIL-ERS) por la infracción del artículo 33 de la LOPD (hoy, artículos 44 del RGPD y 40 de la LOPDGDD).

**2)** Transferencias internacionales de datos mediante garantías adecuadas (Resolución de archivo de las actuaciones practicadas por la Agencia Española de Protección de Datos ante la entidad UNIVERSIDAD COMPLUTENSE DE MADRID, de fecha 21 de septiembre de 2018) [26].

D. *A.A.A.* (en lo sucesivo el denunciante) formula denuncia contra la entidad UNIVERSIDAD COMPLUTENSE DE MADRID (en lo sucesivo UCM), en la que se matriculó para el curso académico 2016/2017. En concreto, se refiere el denunciante a diversas circunstancias que derivan del contrato de prestación de servicios que la citada Universidad tiene suscrito con la entidad Google Inc. (actualmente Google LLC) para el correo electrónico bajo el dominio *"ucm"*, destinado a la comunidad universitaria,

[26] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-06555-2017.pdf [Fecha de consulta: 26/09/2024].

señalando que la creación de una cuenta de correo en dicho dominio conlleva la aceptación de las condiciones de servicio y la política de privacidad de Google, en la que figura que la finalidad principal es publicitaria y comercial (*"Nuestros sistemas analizan tu contenido para ofrecerte funciones de productos que sean relevantes para ti..."*); que la compañía vincula el contenido de los datos de otros servicios; y que la misma efectúa tratamiento de datos de carácter personal ("*La información que recogemos cuando inicias sesión en Google, además de los datos que obtenemos sobre ti a través de nuestros partners, se puede asociar a tu cuenta de Google. Cuando la información se asocia a tu cuenta de Google la tratamos como información personal"*).

El denunciante manifiesta que la UCM no informa en la matrícula de los alumnos de todos estos hechos, únicamente de una colaboración con Google a partir de octubre de 2012 ("*El objetivo de esta iniciativa es ofrecer a la comunidad universitaria una serie de servicios en la nube. Entre ellos un buzón de correo de 25GB"*), sin especificar otros aspectos como el destino de los datos, ubicación de los servidores o los responsables de los tratamientos. Así mismo manifiesta que la UCM tampoco informa sobre el procedimiento para ejercer los derechos.

Por otra parte, añade que es requisito indispensable para tener una cuenta de correo introducir una clave proporcionada por la propia Universidad y seguir los pasos establecidos por la UCM en su web (http://www.ucm.es), entre los que figura la *Gestión de la Identidad UCM* y dentro de ella, las *"Condiciones de uso"* de las cuentas de correo, en la que consta como finalidad la utilización para fines académicos y otros de carácter personal o privado legal y no comercial. En los principios generales también figura que se prohíbe el envío de "spam", los envíos masivos y que a través de la cuenta se podrán recibir las comunicaciones de la UCM.

El denunciante manifiesta que esta información solo se refiere a la Gestión de Identidad UCM y no a las condiciones de utilización de correo electrónico que corresponden a las condiciones de Google, lo que supone una recogida de datos en forma engañosa o fraudulenta ya que los datos se almacenan en Estados Unidos.

El presente procedimiento se circunscribe a determinar la regularidad de los servicios "G Suite para Educación" de Google habilitados por la UCM con destino a la comunidad

universitaria, entre los que se incluye el servicio Gmail (correo electrónico) al que se refiere el denunciante.

Las garantías ofrecidas en estas contrataciones de servicios de computación en nube prestados por Google, fue analizada, con carácter general, por el Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE (hoy Comité Europeo de Protección de Datos –artículos 68 a 76 del RGPD–), en el marco del procedimiento establecido en el documento de trabajo 226, a partir de las cláusulas contractuales tipo adoptadas por la Comisión Europea en su Decisión 2010/87/UE y de los acuerdos suplementarios o cláusulas adicionales que pudieran incluirse para adaptar las garantías a las especificidades de la prestación de servicios en el contexto de la computación en la nube.

En el citado documento de trabajo 226 se analizaron los documentos "Términos y Condiciones de Seguridad y Tratamiento de Datos" y "Contrato de la Adenda de Tratamiento de Datos" y, con fecha 30/12/2016, el Grupo del artículo 29 consideró que tales documentos cumplían con los requisitos de la Decisión de la Comisión Europea sobre cláusulas contractuales tipo para la transferencia internacional de datos 2010/87/UE, de 5 de febrero de 2010. El resto de los servicios adicionales que Google proporciona, no incluidos en los servicios "G Suite para Educación", se regulan por la política de privacidad y las Condiciones de uso de Google. Sin embargo, estos servicios adicionales pueden ser activados o desactivados por los usuarios. Estas circunstancias se expresan claramente por parte de la Universidad a los alumnos y trabajadores para los que se habilitaron los servicios objeto de las actuaciones. Así, en el proceso de alta, estos usuarios deben aceptar las condiciones de uso redactadas por el Departamento de Seguridad, en las que se informa, entre otros aspectos, que solo se podrán utilizar estos servicios para *"fines académicos y otros de carácter personal o privado legal y no comercial"*. Asimismo, se informa sobre la política de privacidad, detallando que el responsable del fichero es el Vicerrectorado de Informática y Comunicaciones de la Universidad, así como la finalidad y el procedimiento para ejercer los derechos. Asimismo, la primera vez que el usuario accede a la cuenta recibe un mensaje de bienvenida y se le advierte que el acceso a los servicios de *G. Suite* se rigen por el acuerdo formalizado por la UCM y que la cuenta creada es compatible con muchos servicios de Google, los cuales, sin son distintos a los habilitados por el administrador, están regulados por las Condiciones de Servicio de Google y la Política de Privacidad de Google.

Por lo tanto, de acuerdo con lo señalado, la Directora de la Agencia Española de Protección de Datos acuerda proceder al archivo de las presentes actuaciones.

**3)** Aplicación territorial de la normativa española en materia de protección de datos en el marco de las actividades de un establecimiento del responsable del tratamiento en territorio español o cuando se han empleado medios situados en España por parte de un responsable del tratamiento no establecido en la UE (Procedimiento sancionador PS/00541/2010 a las entidades GOOGLE Inc. (actualmente GOOGLE LLC) y GOOGLE SPAIN, S.L, de fecha 6 de noviembre de 2017) [27].

Entre los servicios ofrecidos por la entidad GOOGLE LLC figura el denominado "Google Street View" que, como complemento del servicio "Google Maps", permite observar imágenes de las calles y carreteras de numerosos países del mundo, entre los que se encuentra España.

La recogida de información para el "Proyecto Google Street View" se inició en España en mayo de 2008, habiendo recorrido aproximadamente el 80% de las vías públicas en el territorio peninsular, con una cobertura casi completa de todas las ciudades con una población igual o superior a 100.000 habitantes. Esta campaña de recogida de datos se paralizó el 10 de mayo de 2010.

Las imágenes que utiliza el servicio "Google Street View" son captadas por una flota de vehículos que recorren las carreteras y calles del territorio de que se trate. Estos vehículos disponen de un equipamiento instalado por GOOGLE LLC sin el concurso de terceros, compuesto por nueve cámaras fotográficas, un ordenador, un switch o conmutador (dispositivo que permite conectar las cámaras al ordenador), un dispositivo GPS, un dispositivo de comunicación inalámbrico conectado a una antena externa que permite la recogida de las señales emitidas por las redes inalámbricas próximas al vehículo, un modem para descargar y actualizar las versiones del software utilizados por el ordenador del vehículo (el programa ***SOFTWARE.2) y un conjunto de discos duros extraíbles en los que se guarda la información captada.

[27] *Vid*. Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/ps-00541-2010.pdf [Fecha de consulta: 26/09/2024].

El ordenador tiene instalado un software utilizado para captar tres tipos de información: imágenes, información de posicionamiento e información trasmitida por redes inalámbricas. Contiene un programa denominado ***SOFTWARE.1 que, mediante la antena dispuesta al efecto, capta e interpreta las señales de redes inalámbricas, traduciéndolas a un conjunto de datos inteligibles y útiles como, por ejemplo, las direcciones IP de origen y destino, el SSID de la red mediante la que se ha transmitido la trama, la fuerza de la señal recibida, etc. La información captada por la antena GPS y el programa ***SOFTWARE.1 es comunicada a un programa desarrollado por GOOGLE LLC, denominado "***SOFTWARE.2", que procesa la información recogida y la guarda en una serie de ficheros en el disco duro. Este programa "***SOFTWARE.2", dispone de opciones que permiten configurar, al ejecutarlo, qué tipo de tramas serán almacenadas, pudiendo incluir o excluir por separado los distintos tipos de tramas, así como los cuerpos de las tramas cifradas (los Servicios de Inspección de la AEPD verificaron que el funcionamiento del sistema ***SOFTWARE.2 puede configurarse con una opción disponible "— discard_data_frame", que permite descartar las tramas de tipo DATA recogidas de las redes no cifradas).

El sistema informático almacenaba la información captada en tres ficheros: uno para las imágenes captadas por las cámaras, otro para datos del sistema GPS y un tercero, generado por el programa ***SOFTWARE.2, para los datos de redes inalámbricas.

La recogida de información efectuada en España para el "Proyecto Google Street View" durante los años 2008, 2009 y 2010 incluía, además de imágenes y datos del sistema GPS, la información transmitida públicamente por redes inalámbricas (Wifi), en concreto, direcciones MAC del router y dispositivos conectados, SSID o nombre de la red (...).

Procede en este supuesto analizar el ámbito de aplicación territorial de la LOPD respecto de los hechos imputados; cuestión de la que se derivan dos aspectos básicos como son la posible existencia o no de infracciones y la propia competencia de la Directora de la AEPD para, en su caso, declararlas e imponer las sanciones legalmente previstas. El examen de esta cuestión exige considerar si las conductas analizadas han sido llevadas a cabo en el marco de las actividades de un establecimiento del responsable del tratamiento en territorio español o se han empleado medios situados en España por parte de un responsable del tratamiento no establecido en la Unión Europea. Si nos encontrásemos en

uno de estos casos serían aplicables los principios, derechos y garantías previstos en la legislación española de protección de datos.

Conforme a lo dispuesto en el artículo 4.1.a) de la Directiva 95/46/CE (hoy, artículo 2 del RGPD), la aplicación de las disposiciones nacionales de un Estado miembro viene determinada por la existencia de un establecimiento del responsable del tratamiento en el territorio del Estado miembro de que se trate. Aunque esta Directiva no define el concepto de "establecimiento", en su preámbulo (Considerando 19) y sí lo hace el artículo 3 del RGPD, señala como elemento determinante el ejercicio efectivo y real de actividades a través de una instalación estable, no siendo preciso que dicho establecimiento tenga personalidad jurídica. Además, el tratamiento de datos personales deberá llevarse a cabo en el marco de tales actividades (= "establecimiento principal").

Por tanto, se ha de tener en cuenta el lugar en que efectivamente se encuentre ubicado el establecimiento del responsable en cuyo contexto se lleva a cabo el tratamiento de los datos, al ser su intervención necesaria para que dicho tratamiento llegue a tener lugar.

En los Antecedentes se describe detalladamente la participación de GOOGLE SPAIN en los hechos, que tiene relación directa con la recogida de datos personales en todo el territorio español. Para que dicha recogida de datos se pudiera llevar a efecto, GOOGLE SPAIN suscribió en su propio nombre un contrato de encargo del tratamiento con EUROVENDEX, en virtud del cual dispuso los vehículos equipados con la tecnología necesaria, indicó las áreas a cubrir, facilitó la formación inicial del personal de EUROVENDEX, designó las personas de contacto, realizó el pago de las facturas generadas por el servicio y asumió la responsabilidad de cumplir en todo el proceso con las obligaciones legales establecidas en la LOPD, exigiendo la implantación de las medidas de seguridad de nivel medio establecidas en la normativa de protección de datos.

Dado que las investigaciones realizadas por la Inspección de Datos de la AEPD acreditan suficientemente que el tratamiento de datos consistente en la recogida de datos personales llevada a cabo por los vehículos empleados en el proyecto "Google Street View" ha sido realizado en el marco de las actividades de un establecimiento del responsable del tratamiento ubicado en territorio español, cabe concluir que la protección conferida por la LOPD es aplicable al presente supuesto y, por ende, la AEPD es competente para la

tramitación del presente procedimiento, de conformidad con lo establecido en el artículo 2.1.a) de la citada Ley Orgánica.

Como ya se ha señalado anteriormente, la existencia de un "establecimiento" supone el ejercicio real y efectivo de actividades a través de gestiones estables, y la forma jurídica del establecimiento (una oficina local, una filial con personalidad jurídica o una representación mediante terceros) no resulta determinante. En este caso, al margen de la forma jurídica de la entidad GOOGLE SPAIN, puede entenderse que existe un establecimiento implicado en actividades que entrañan el tratamiento de datos personales relativos a personas identificadas o identificables, que se recaban, se tratan y divulgan en territorio español. GOOGLE SPAIN es el establecimiento de Google en cuyo contexto se tratan los datos.

Por lo tanto, cabe concluir que la protección conferida por la normativa española en materia de protección de datos es aplicable al presente supuesto y, por ende, la AEPD es competente para la tramitación del presente procedimiento, de conformidad con lo establecido en el artículo 2.1.a) de la LOPD (hoy, artículos 3 del RGPD y 2 de la LOPDGDD), en la medida en que GOOGLE LLC ha recurrido a medios situados en el territorio español, como son los equipos instalados en los vehículos empleados en el proyecto "Google Street View", con el fin de captar información en nuestro territorio. En este caso, la utilización de tales equipos para la recogida de datos no se realiza exclusivamente con fines de tránsito por el territorio de la Unión Europea, es decir, no se trata de equipos de transmisión, sino que dichos equipos se emplean para la recogida y tratamiento de los datos.

**4)** Vulneración del derecho de información y acceso a los datos personales en relación con una transferencia internacional de datos (Resolución de archivo de actuaciones ante las entidades AEROVIAS DE MEXICO SA DE C.V. (AEROMEXICO), AIR EUROPA LINEAS AEREAS SA, IBERIA LINEAS AEREAS DE ESPAÑA SOCIEDAD ANONIMA OPERADORA en virtud de denuncia presentada por FACUA - CONSUMIDORES EN ACCIÓN, de fecha 3 de octubre de 2013) [28].

[28] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-06406-2012.pdf [Fecha de consulta: 26/09/2024].

Con fecha 24 de septiembre de 2012 se recibió, en la AEPD, un escrito de la Asociación de Consumidores y usuarios en Acción FACUA en relación a los vuelos con destino a Toronto, Montreal, México DF y La Habana que sobrevuelan el espacio aéreo estadounidense, pero sin realizar escalas en su territorio, en el que denuncia a las compañías aéreas AEROVIAS DE MÉXICO SA DE C.V. (AEROMÉXICO), AIR EUROPA LINEAS AEREAS SA, IBERIA LINEAS AEREAS DE ESPAÑA SOCIEDAD ANONIMA OPERADORA por las siguientes conductas: 1) la comunicación de datos de los pasajeros de dichos vuelos a las autoridades de Estados Unidos sin el consentimiento de los sujetos; 2) incumplir el principio de calidad de datos al ser los datos comunicados no pertinentes y excesivos; y, 3) no informar a sus pasajeros de que sus datos serán suministrados a Estados Unidos en el momento de la contratación de dichos vuelos.

AEROMÉXICO

AEROMÉXICO manifiesta que la información que se suministra a los pasajeros con anterioridad a recabar sus datos personales se encuentra:

- En la página web de AEROMÉXICO, (www.aeromexico.com), en donde se les comunica que por disposición de la Administración para la Seguridad en el Transporte de los Estados Unidos (TSA) se implementa la norma "Secure Flight" para vuelos desde y hacia dicho país. Igualmente, se les informa de la obligación de aportar los datos personales solicitados para poder efectuar la reserva del vuelo.
    - AEROMÉXICO ha aportado copia de la información que aparece reflejada en su web (www.aeromexico.com) en la que figura: *Aeroméxico informa a todos sus Agentes de Viaje que por disposición de la Administración de Seguridad en el Transporte Aéreo de Estados Unidos (TSA por sus siglas en inglés) y efectivo a partir del 08 de Mayo de 2012, todas las reservaciones que contengan algún segmento de vuelo desde o hacia o que sobrevuele Estados Unidos de América deben incluir de forma obligatoria, la información requerida por la TSA que consiste en: Nombre completo del cliente, tal y como aparece en el pasaporte, Fecha de nacimiento (DD/MM/AA) y Género*.

- *Estos elementos deben ser incluidos antes de finalizar la reservación y emisión del boleto a través de un SSRDOCS para cada uno de los clientes que conforman la reservación, incluyendo infantes. A partir del 08 de mayo de 2012, todas las reservaciones de vuelos desde o hacia y que sobrevuelen Estados Unidos de América que no reporten la información de Secure Flight serán rechazadas por TSA, negando el ingreso o sobrevuelo a los Estados Unidos de América por no reportar el Secure Flight en su reservación…*

- En el CALL CENTER: Se informa a los clientes en el momento de realizar su reserva.

- En el Aeropuerto: Se informa a los clientes con carteles en los mostradores de ventas y *check in*.

- A través de las Agencias de Viajes: Se editó un comunicado, en fecha 4 de mayo de 2012, que se envió a todas las agencias de viajes españolas. AEROMEXICO ha aportado copia de dicho comunicado que es similar al que figura en la web, incluyendo, además el siguiente texto: *Por lo anterior, les informamos que a partir de la fecha de este comunicado aquellas reservaciones de vuelos de Aeroméxico, Aeroméxico Connect o en Código Compartido con código AM operados por otras aerolíneas desde o hacia o sobrevolando Estados Unidos de América que no presenten la información de Secure Flight, y que por consecuencia sean rechazadas, Aeroméxico tendrá que aplicar los cargos correspondientes para su reinstalación una vez que se ingrese la información requerida. Asimismo, solicitamos su apoyo en revisar todas las reservaciones que no cuenten con el SSRDOCS correspondiente, reservaciones preexistentes que hayan realizado previas a la fecha en que les notificamos la norma de Secure Flight. Favor de contactar a su cliente, solicitar e ingresar la información necesaria en la reservación de vuelos. Los formatos para ingresar el SSRDOCS en las reservaciones varían de acuerdo con su Globalizador. En caso de tener alguna duda o desconocer los formatos para ingresar el SSRDOCS, deberá contactar a la mesa de ayuda de su Globalizador. Recuerda informarle al cliente que es un requerimiento mandatario de la Autoridad Americana de Seguridad*

*TSA y la importancia de incluir sus datos correctamente en su reservación la información que aparece reflejada en su web www.aeromexico.com.*

AEROMÉXICO manifiesta que, desde el pasado 24 de junio de 2010, se incluye dicha información en cada reserva realizada para los vuelos que sobrevuelan los EE.UU. en un campo denominado SSRDOCS (SECURE FLIGHT), con al menos setenta y dos horas de antelación a la salida del vuelo con la siguiente información de cada cliente: nombre completo (según aparece en el pasaporte), género y fecha de nacimiento.

Asimismo, manifiesta que setenta y dos horas antes de la salida del vuelo, el sistema de reservas SABRE envía de forma automática la información de *Secure Flight* de cada cliente a la base de datos de TSA (*Transportation Security Administration*) para que sea validada por ésta. En el caso de que se generen nuevas reservas dentro de esas setenta y dos horas, el sistema SABRE enviará automáticamente la información *Secure Flight* de la nueva reserva para su validación por TSA. En caso de que la información no esté presente en la reserva a la hora de retirar su tarjeta de embarque para el vuelo, el agente de facturación ingresa la información y ésta es transmitida automáticamente a la base de datos de TSA para su validación.

AEROMÉXICO informa, con el siguiente texto, y que se puede consultar accediendo a los enlaces de la web de TSA: www.tsa.gov/secureflight y www.tsa.gov, que igualmente figuran indicados en la página informativa de AEROMÉXICO: *En cumplimiento con el título 49 US.C. sección 114 de la Reforma de Inteligencia y Prevención de Actos Terroristas de 2004 así como el título 49 C.F.R. partes 1540 y 1560, la Administración de Seguridad del Transporte (TSA por sus siglas en inglés), requiere que proporcione su nombre completo, fecha de nacimiento y género con el propósito de realizar una revisión. Usted podrá proporcionar su número de compensación si lo tiene disponible. Algún error al proporcionar su nombre completo, fecha de nacimiento y género, podría resultar en negarle el transporte o la Autoridad podrá negarle la entrada a la sala de abordaje. La TSA puede compartir la información que usted proporciona con agencias de inteligencia u otras bajo su sistema de aviso. Si requiere más información acerca de las políticas de privacidad de TSA o revisar el sistema de avisos, por favor visite el sitio Web de TSA: www.tsa.gov.*

AIR EUROPA LINEAS AEREAS SA

AIR EUROPA manifiesta que cuando una persona compra un billete aéreo con la compañía, en el momento de recabar sus datos, se le remite a la política de privacidad de la Compañía. Durante el proceso de la reserva, en el caso de hacerla con origen o destino a los EE. UU., Reino Unido o Cuba, o que se sobrevuele el espacio aéreo de EE. UU., se le informa que, en este caso, según las instrucciones de las autoridades de esos países, se está obligado a incluir el nombre y apellidos de los pasajeros, además de incluir la fecha de nacimiento.

A este respecto AIR EUROPA ha aportado impresiones de pantalla del proceso de reserva en las que figura el siguiente texto: *Está usted haciendo una reserva con origen o destino EE.UU., REINO UNIDO o CUBA. También puede estar haciendo una reserva con un vuelo que sobrevuele el espacio aéreo de EE. UU. Por esta razón y siguiendo instrucciones de las autoridades de esos países está obligado a: incluir el nombre y apellidos de los pasajeros que coincidan exactamente con los que aparezcan en sus respectivos pasaportes. No vale usar ni diminutivos, ni iniciales, ni traducciones si éstas no están de esa manera en el mismo pasaporte, incluir datos extra: fecha de nacimiento*.

AIR EUROPA manifiesta que los oficiales del Departamento de Seguridad Nacional de los Estados Unidos pueden acceder a los datos concernientes a los viajeros a bordo (pasajeros, miembros de equipo, y, a veces, miembros del "non crew") de los vuelos de la compañía AIR EUROPA, que llegan, salen, y sobrevuelan el espacio aéreo de los Estados Unidos. Los mismos, no tienen acceso a las reservas, solo tienen acceso a los datos que la compañía AIR EUROPA les envía vía SITA, de manera codificada. Para esto, existe una Instrucción facilitada a AMADEUS, para que se realice dicha acción.

La tipología de los datos concretos a los que se accede, como se especifica en el documento de las Autoridades Americanas "APIS Pre-Departure Final Rule", se deben enviar completos y cumplimentados antes del cierre de puertas del avión. Estos datos incluyen los siguientes campos: datos del vuelo (número de vuelo, fecha y hora de salida, origen y destino), datos de los pasajeros (número de documento de viaje, apellido, nombre, fecha de nacimiento, fecha en que expira el documento, nacionalidad, sexo, país que emite el documento, país de residencia, dirección en los Estados Unidos (número/calle/código postal/ciudad).

AIR EUROPA manifiesta que para comenzar a operar en vuelos a Estados Unidos y/o sobrevolar su Espacio Aéreo, ha implementado todos los procedimientos de acuerdo con las instrucciones de la Agencia Estatal USA. Las bases que permiten que los Oficiales del Departamento de Seguridad Nacional de los Estados Unidos acceder a los datos de los pasajeros, están reguladas sobre:

- Requerimientos que solicitan por parte de las autoridades americanas (APIS *Pre-Departure Final Rule* 080307).
- Capítulo 2 del Programa Nacional de Seguridad USA. (Extracto del Capítulo 2 *apis. -secureflight*)
- Documento donde se confirma que las medidas en el MSP (Programa de Seguridad), se aplicarán por parte de la compañía AIR EUROPA. (*Foreign Air carrier Security programme*).
- Documento en donde se confirma la lectura y aplicación de las medidas de seguridad USA, por parte de la compañía. (*Check list begining Ops to USA*.).

AIR EUROPA manifiesta que en el convenio sobre aviación civil internacional realizado en Chicago el 7 de diciembre de 1944, Instrumento de ratificación de 21 de febrero de 1947 (BOE de 24 de febrero de 1947), texto auténtico ratificado por España mediante instrumento de fecha de 18 de marzo de 1969 (BOE de 29 de diciembre de 1969), en sus artículos 1 y 2, "*Soberanía y Territorio*", del Capítulo 1. Principios generales y aplicación del Convenio, se establece: "*Artículo 1. Soberanía: Los Estados contratantes reconocen que todo Estado tiene soberanía plena y exclusiva en el espacio aéreo situado sobre su territorio. Artículo 2. Territorio: A los fines del presente Convenio se consideran como territorio de un Estado las áreas terrestres y las aguas territoriales adyacentes a ellas que se encuentren bajo la soberanía, dominio, protección o mandato de dicho Estado*."

AIR EUROPA manifiesta que, con carácter general, cuando un pasajero compra un billete a la Compañía Air Europa, y ese vuelo lo opera otra compañía, ya sea en código compartido, *subcharter* o *wet lease*, la información ofrecida a dicho pasajero es exactamente la misma que cuando un vuelo es operado por AIR EUROPA, pero con información adicional de la compañía operadora.

IBERIA LINEAS AEREAS DE ESPAÑA SOCIEDAD ANONIMA OPERADORA

IBERIA manifiesta que, dentro del proceso de compra de billetes, se solicita al usuario la aceptación de los términos y condiciones correspondientes al país de navegación en el que esté realizando la compra, condiciones a las que puede acceder en cualquier momento y que deben ser expresamente aceptadas por el pasajero para completar la compra.

En el caso de seleccionar un vuelo que sobrevuele el espacio aéreo de los Estados Unidos, por ejemplo, con destino a México D.F., se muestra un mensaje destacado en la parte superior de la pantalla en la que se recaban los datos personales durante el proceso de compra con el siguiente texto:

*Estás reservando un vuelo que sobrevuela el espacio aéreo de EE. UU. En cumplimiento de la legislación vigente, deben recabarse y cederse a EE. UU. ciertos datos de carácter personal. Para más información consulta la política de protección de datos y seguridad de la información.*

La frase subrayada es un enlace que conduce a la política de protección de datos y seguridad de la información de IBERIA, en la que explícitamente se señala:

*Asimismo le informamos que, en cumplimiento del requerimiento expreso efectuado a todas las compañías aéreas por motivos de control y salvaguarda de la seguridad pública, Iberia estará facultada a comunicar sus datos como pasajero a las Autoridades Gubernamentales de Control de la Seguridad Interna del país de origen, tránsito o destino en cualquier momento antes de su llegada, con dicha finalidad. Estados Unidos exige también esta información para los aviones que sobrevuelen su espacio aéreo. Esta información también podrá ser facilitada también a otros Estados que, en virtud de lo dispuesto en las leyes o tratados aplicables, exijan la misma para el sobrevuelo de su espacio aéreo.*

*(…)*

*La recolección de ciertos datos personales es indispensable para realizar la Reserva y establecer el Contrato de Transporte. Naturalmente, el Pasajero puede ejercer su derecho de oposición a la recolección y al tratamiento de estos datos, pero se le informa que esto podría provocar la cancelación del viaje o la imposibilidad de acceder a ciertos servicios anexos específicos solicitados (comidas especiales, etc.). Asimismo, cabe*

*recordar que, en conformidad con las leyes y reglamentos aplicables en España y a nivel internacional, el hecho de no comunicar ciertos datos o de comunicar datos inexactos podría conducir a una decisión de denegación de embarque o de entrada a un territorio extranjero, sin que el Transportista pueda ser considerado responsable por este particular.*

IBERIA ha aportado Notificación, de fecha 18 de julio de 2011, informando de la implementación del Programa SF/Overflights en el plazo de 180 días y Guía Técnica Operativa para su implementación (TSA *Secure Flight*, 18 de julio de 2011). En dichos documentos constan las directrices operacionales y técnicas para los sobrevuelos en el espacio aéreo de EE. UU. por compañías aéreas extranjeras.

Entre ellos, se exige a las compañías aéreas extranjeras presentar el *Secure Flight Passenger Data* (SFPD) para los pasajeros 72 horas antes de la salida del vuelo en los vuelos que sobrevuelan, pero no aterrizan en el territorio continental de Estados Unidos, cuando ese país es Canadá o México. TSA determinó la lista inicial de pares de aeropuertos.

TSA requerirá los siguientes datos: nombre, fecha de nacimiento, sexo, e información de itinerario y del pasaporte, 72 horas antes de la salida programada del vuelo. Las compañías aéreas extranjeras deben remitir a TSA las modificaciones realizadas en cualquiera de los datos de pasajeros o la información de reservas de vuelo en el momento en que la compañía aérea extranjera hace las modificaciones.

IBERIA ha aportado documento del cambio 16 del *Model Security Program* para transportistas extranjeros, de fecha 8 de febrero de 2012, y con fecha de efectividad 8 de marzo de 2012.

En el presente caso se denuncia la falta del derecho de información con relación a la transferencia de datos a las autoridades norteamericanas. El artículo 5 de la LOPD (hoy, artículos 13 y 14 del RGPD y 11 de la LOPDGDD) exige el deber de informar a los afectados de los que se recaban datos como un requisito previo a su tratamiento para que conozcan lo que supone proporcionar los mismos y conozcan los fines y destinos de estos como un medio también de controlar y disponer de sus propios datos. Este derecho de información es objeto de protección por sí mismo.

En el caso de la línea aérea AEROVIAS DE MEXICO SA DE C.V. (AEROMEXICO), se informa a los clientes de los vuelos que cruzan el espacio aéreo de los Estados Unidos sobre la transmisión de los datos API a las autoridades estadounidenses por los diferentes medios antes mencionados.

En el caso de la línea aérea AIR EUROPA LINEAS AEREAS SA, como ya se ha señalado, cuando una persona compra un billete aéreo con la compañía, en el momento de recabar sus datos, se le remite a la política de privacidad de la compañía en donde aparece el siguiente apartado: *Le informamos que conforme a la legislación de algunos países, sus datos personales… pueden ser facilitados al departamento de aduanas o autoridad competente que lo solicita formalmente, si su vuelo tiene origen, destino, escala o sobrevuela alguno de esos países.* Durante el proceso de la reserva, en el caso de hacerla con origen o destino a los EE. UU., Reino Unido o Cuba, o que se sobrevuele el espacio aéreo de EE. UU., se informa a los clientes sobre la transmisión de los datos API a las autoridades correspondientes, donde de forma explícita indica: *También puede estar haciendo una reserva con un vuelo que sobrevuele el espacio aéreo de EE. UU. Por esta razón y siguiendo instrucciones de las autoridades de esos países está obligado a: incluir el nombre y apellidos de los pasajeros que coincidan exactamente con los que aparezcan en sus respectivos pasaportes.*

En el caso de la línea aérea IBERIA LINEAS AEREAS DE ESPAÑA SOCIEDAD ANONIMA OPERADORA, tal y como consta en las actuaciones previas de inspección, se informa a los clientes sobre la transmisión de los datos API a las autoridades estadounidenses. En el caso de seleccionar un vuelo que sobrevuele el espacio aéreo de los Estados Unidos, como ya se ha señalado, se muestra un mensaje destacado en la parte superior de la pantalla en la que se recaban los datos personales durante el proceso de compra con el siguiente texto: *Estás reservando un vuelo que sobrevuela el espacio aéreo de EE. UU. En cumplimiento de la legislación vigente, deben recabarse y cederse a EE. UU. ciertos datos de carácter personal. Para más información consulta la política de protección de datos y seguridad de la información*.

La frase subrayada es un enlace que conduce a la política de protección de datos y seguridad de la información de IBERIA, en la que explícitamente se señala:

*Asimismo, le informamos que, en cumplimiento del requerimiento expreso efectuado a todas las compañías aéreas por motivos de control y salvaguarda de la seguridad pública, Iberia estará facultada a comunicar sus datos como pasajero a las Autoridades Gubernamentales de Control de la Seguridad Interna del país de origen, tránsito o destino en cualquier momento antes de su llegada, con dicha finalidad. Estados Unidos exige también esta información para los aviones que sobrevuelen su espacio aéreo. Esta información también podrá ser facilitada también a otros Estados que, en virtud de lo dispuesto en las leyes o tratados aplicables, exijan la misma para el sobrevuelo de su espacio aéreo.*

*(…)*

*La recolección de ciertos datos personales es indispensable para realizar la Reserva y establecer el Contrato de Transporte. Naturalmente, el Pasajero puede ejercer su derecho de oposición a la recolección y al tratamiento de estos datos, pero se le informa que esto podría provocar la cancelación del viaje o la imposibilidad de acceder a ciertos servicios anexos específicos solicitados (comidas especiales, etc.). Asimismo, cabe recordar que, en conformidad con las leyes y reglamentos aplicables en España y a nivel internacional, el hecho de no comunicar ciertos datos o de comunicar datos inexactos podría conducir a una decisión de denegación de embarque o de entrada a un territorio extranjero, sin que el Transportista pueda ser considerado responsable por este particular.*

Por tanto, el Director de la AEPD acuerda proceder al archivo de las presentes actuaciones.

**5)** Caducidad de las actuaciones en el ejercicio del derecho de acceso dentro del marco de las transferencias internacionales de datos (Resolución de caducidad de actuaciones ante la autoridad de protección de datos de Países Bajos contra BANKINTER, S.A., de fecha 14 de junio de 2022[29]).

D. A.A.A. (en adelante, la parte reclamante) interpuso reclamación ante la autoridad de protección de datos de Países Bajos. La reclamación se dirige contra BANKINTER, S.A.,

[29] *Vid.* Procedimiento sancionador completo disponible en: https://www.aepd.es/es/documento/e-02670-2020.pdf [Fecha de consulta: 26/09/2024].

con NIF A28157360 (en adelante, BANKINTER). Los motivos en que basa la reclamación son los siguientes: la parte reclamante ejercitó su derecho de acceso ante BANKINTER, recibiendo respuesta, en fecha 4 de febrero de 2019, indicando que no constaba en sus registros como cliente o excliente.

Junto con la reclamación aporta: a) copia de un correo electrónico de la parte reclamante a privacidad@bankinter.com, de fecha 29 de enero de 2019, en el que manifiesta que adjunta su solicitud de acceso a sus datos personales en PDF; b) copia de un documento firmado por la parte reclamante, de fecha 29 de enero de 2019, en el que solicita a BANKINTER el acceso a sus datos personales; c) copia de un correo electrónico desde privacidad@bankinter.com a la parte reclamante, de fecha 31 de enero de 2019, en el que se le informa de que se ha trasladado su petición al departamento correspondiente, desde el que se le dará cumplida respuesta en el plazo y forma establecidos; d) copia de un documento de BANKINTER, de fecha 4 de febrero de 2019, dirigido a la parte reclamante, en el que se le informa que no pueden atender a su solicitud de acceso ya que sus datos no figuran en sus registros como cliente o excliente de la entidad; e) copia de un correo electrónico de la parte reclamante a privacidad@bankinter.com, de fecha 12 de febrero de 2019, en el que informa: "Buenas tardes, Recibida vuestra respuesta por correo en el día de hoy (adjunto), en la que se niega que tenga algún producto contratado con ustedes, indicar que no es cierto, ya que tengo una cuenta abierta con ustedes (***CUENTA.1). Adjunto documento emitido por ustedes en referencia a esta cuenta. Ruego por tanto revisen de nuevo sus registros y procedan con la solicitud. Un saludo."; f) copia de un documento de BANKINTER, de fecha septiembre de 2017, dirigido a la parte reclamante, en el que se le envía la información relativa a sus operaciones con Bankinter, necesaria para cumplimentar su declaración de impuestos correspondiente al ejercicio de 2016, en el que figura que la parte reclamante es titular de la cuenta número ***CUENTA.1; y, g) copia de un correo electrónico de privacidad@bankinter.com a la parte reclamante, de fecha 14 de febrero de 2020, en el que se le informa: "Trasladamos su solicitud al departamento correspondiente, desde el que se le dará cumplida respuesta en el plazo y forma establecidos".

En fecha 7 de febrero de 2020, tuvo entrada en la AEPD la citada reclamación, a través del "Sistema de Información del Mercado Interior" (en lo sucesivo, IMI), regulado por el Reglamento (UE) N.º 1024/2012, del Parlamento Europeo y del Consejo, de 25 de octubre

de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información. El traslado de esta reclamación a la AEPD se realizó de conformidad con lo establecido en el artículo 56 del RGPD, teniendo en cuenta su carácter transfronterizo y que la AEPD es competente para actuar como autoridad de control principal, dado que BANKINTER tiene su sede social y establecimiento único en España.

Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, actúa en calidad de "autoridad de control interesada", además de la autoridad de protección de datos de Países Bajos, la autoridad de Portugal. Esta última en virtud del artículo 4.22 del RGPD, dado que los interesados que residen en este país es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

Con fecha 3 de julio de 2020, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 RGPD, y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos: en respuesta a requerimiento de información de esta Agencia, en fecha 30 de abril de 2020, los representantes de BANKINTER manifiestan que disponen de procedimientos y mecanismos adecuados para dar cumplimiento a la tramitación de los derechos de protección de datos de los interesados. Aportan copia del procedimiento.

En relación con el motivo por el que la respuesta facilitada a la parte reclamante como consecuencia de su ejercicio del derecho de acceso en que no figuraba información relativa a la cuenta ***CUENTA.1, los representantes de la entidad indican que se produjo un error puntual en la aplicación del Procedimiento de Derechos. Ello hizo que no se localizase e identificase dicha cuenta como correspondiente a la parte reclamante, por lo que BANKINTER no le facilitó tal información.

En fecha 20 de abril de 2020, el error se ha solventado, habiéndose dado contestación al derecho de acceso de la parte reclamante de forma completa. Los representantes de la

entidad aportan copia del correo electrónico remitido a la parte reclamante con la información solicitada en un documento adjunto cifrado.

De conformidad con lo expuesto, la AEPD declaró que, en relación con las actuaciones previas, el Reglamento de desarrollo de la LOPD (RLOPD), aprobado por Real Decreto 1720/2007, de 21 de diciembre, en vigor en todo aquello que no contradiga, se oponga o resulte incompatible con lo dispuesto en el RGPD y en la LOPDGDD, en su artículo 122.4 dispone que: "El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas".

A tenor de lo dispuesto en los artículos transcritos, las actuaciones previas han de entenderse caducadas si, transcurridos más de doce meses contados desde la fecha de admisión a trámite de la reclamación, no se ha procedido a dictar y notificar el acuerdo de inicio de procedimiento sancionador.

En el presente supuesto el cómputo de los doce meses de duración máxima de las actuaciones previas E/02670/2020 se inició el día 3 de julio de 2020 y, en aquella fecha, aún estaban pendientes de finalización, por lo que debían declararse caducadas.

Por lo tanto, y de acuerdo con lo señalado, la Directora de la AEPD, acuerda declarar la caducidad de las presentes actuaciones.

## III. REFLEXIÓN FINAL.

Las transferencias internacionales de datos de carácter personal y el diseño de una normativa reguladora adecuada, efectiva y eficaz, que tienda a la protección del titular del derecho a la protección de datos, constituyen un auténtico desafío. Y ello por varios motivos: a) en primer lugar, por la creciente dimensión económica que está cobrando el libre tránsito de la información. El acceso y uso de la información por parte de empresas, administraciones e individuos se ha convertido en un precioso bien intangible, causa y efecto, a la vez de la progresiva integración económica y social; b) en segundo lugar, porque junto a la dimensión económica, la protección de los datos personales y de la intimidad supone afrontar, por vez primera, la difícil tarea de compatibilizar los derechos fundamentales con el comercio internacional. Todo ello en cada una de las distintas esferas jurídicas implicadas; y, c) en tercer lugar, porque

la especial volatilidad de las transferencias internacionales de datos complica extraordinariamente la definición del derecho sustantivo aplicable.

Dicho lo cual, las transferencias internacionales de datos no son una materia exenta del poder sancionador de la AEPD. No obstante, en los últimos años (2010-2024), han sido (en comparación con otras materias) "escasos" los procedimientos sancionadores abiertos por la AEPD; dirigidos, fundamentalmente, contra Administraciones Públicas y entidades (Asociaciones, Fundaciones, empresas de telecomunicaciones, del sector bancario y del sanitario); y fundamentados, todos ellos, en el incumplimiento de los principios de base en materia de transferencia internacional de datos (p. ej., entre otros, por vulneración del principio general de las transferencias internacionales de datos; en casos de transferencias internacionales de datos mediante garantías adecuadas; por aplicación territorial de la normativa española en materia de protección de datos en el marco de las actividades de un establecimiento del responsable del tratamiento en territorio español o cuando se han empleado medios situados en España por parte de un responsable del tratamiento no establecido en la UE; o por vulneración del derecho de información y acceso a los datos personales en relación con una transferencia internacional de datos) con un resultado favorable, en la mayoría de los supuestos, para la parte denunciada.

Así las cosas, en nuestra opinión, el régimen jurídico en materia de transferencia internacional de datos se encuentra a salvo del poder sancionador de nuestra Autoridad de control: a) bien porque no está en el "punto de mira" (de la AEPD); b) bien porque el cumplimiento de las previsiones normativas (recogidas en el RGPD y en la LOPDGDD) está en la "hoja de ruta del principio de autorresponsabilidad" de las Administraciones públicas, instituciones y entidades que recogen, almacenan, tratan y/o transfieren datos de carácter personal fuera del territorio nacional.

En definitiva, la AEPD cuando ha optado por sancionar lo ha hecho no imponiendo multas económicas, sino ordenando, en línea con lo previsto en el artículo 58.2.j) del RGPD, de forma temporal o definitiva, la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional; esto es,

el cese de las transferencias internacionales de datos, hasta que se cumpla con las disposiciones del RGPD.

**BIBLIOGRAFÍA**

DELGADO CARRAVILLA, E y PUYOL MONTERO, J., *La implantación del nuevo Reglamento de Protección de Datos de la Unión Europea*, Tirant lo blanch, Valencia, 2018.

GONZÁLEZ, A. y JEREZ DELGADO, C. (Directores), *Estudios sobre la Jurisprudencia Europea. Materiales del III Encuentro anual del Centro español European Law Institute*, Editorial Jurídica Sepin, Volumen II, Madrid, 2020, pp. 1065-1075.

GUASCH PORTAS, V., *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos-Agencia Estatal Boletín Oficial del Estado, Madrid, 2014.

HANCE, Oliver (1996), "Privacy and the Internet: Intrusion, Surveillance and Personal Data", *International Review of Law Computers & Technology*, vol. 10, Nº 2, pp. 219-234.

LÓPEZ ÁLVAREZ, L.F., *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*, Francis Lefebvre, Madrid, 2016.

LÓPEZ CARBALLO, D., "A vueltas con las transferencias internacionales de datos: actualidad y seguridad jurídica", *Actualidad Jurídica Aranzadi*, núm. 922/2016, Aranzadi, Cizur Menor (Navarra), 2016.

ORTEGA GIMÉNEZ, A.*Transferencias internacionales de datos de carácter personal y el nuevo marco de privacidad de datos UE-EE.UU.*, Editorial COLEX, A Coruña (Galicia), 2023.

ORTEGA GIMÉNEZ, A., "Nuevas cláusulas contractuales tipo para las transferencias internacionales de datos personales a terceros países y entre los responsables y encargados del tratamiento", *La implementación del Reglamento general de protección de datos en España y el impacto de sus cláusulas abiertas*, Editorial Tirant Lo Blanch, Valencia, 2023, pp. 425-446.

ORTEGA GIMÉNEZ, A., "UE vs. EE.UU., tras la STJUE "Schrems II"", en RUDA GONZÁLEZ, A. (Dir.) y L. KUBICA, M. (Coord.), *Estudios sobre Jurisprudencia Europea. Materiales del VI Encuentro anual del Centro español del European Law Institute*, Editorial Jurídica Sepín, Las Rozas, Madrid, 2023, pp. 740-749.

ORTEGA GIMÉNEZ, A., "Teletrabajo y mecanismos adecuados para legitimar transferencias internacionales de datos entre miembros de un mismo grupo empresarial", en ORTEGA GIMÉNEZ, A. (Dir.), HEREDIA SÁNCHEZ, L.S. (Coord.), *Teletrabajo y derecho internacional privado. Problemas y soluciones*, Editorial Aranzadi, S.A.U., Cizur menor, (Navarra), 2023, pp. 21-60.

ORTEGA GIMÉNEZ, A., "El nuevo Marco de Privacidad para las transferencias internacionales de datos de carácter personal con los Estados Unidos", en *LA LEY Privacidad*, Número 17, Editorial LA LEY, Madrid, julio-septiembre 2023, pp.1- 10.

ORTEGA GIMÉNEZ, A., "«A la tercera no va la vencida»: reservas del Comité Europeo de Protección de Datos al nuevo Marco Transatlántico de Privacidad de Datos", en *LA LEY Privacidad*, Nº16, Editorial LA LEY, Madrid, abril-junio de 2023, pp. 1-7.

ORTEGA GIMÉNEZ, A., "¡Goodbye escudo de privacidad! Transferencias internacionales de datos de carácter personal UE-EE.UU., tras la STJUE "SCHREMS II"", en BUENO DE

MATA, F. (Dir.) y GONZÁLEZ PULIDO, I. (Coord.), *FODERTICS 10.0. Estudios sobre Derecho Digital*, Editorial Comares, Albolote (Granada), 2022, pp. 185-194.

ORTEGA GIMÉNEZ, A., "Análisis conceptual de las "transferencias internacionales de datos personales" en España, bajo las enseñanzas del Profesor Miguel Ángel Davara Rodríguez" (Capítulo XV), *Protección de datos: lo que nunca le han contado. Homenaje a Miguel Ángel Davara Rogríguez*, LA LEY, Wolters Kluwer legal & Regulatory España, Las Rozas (Madrid), junio 2022, pp. 237-257.

ORTEGA GIMÉNEZ, A., "Análisis comparado de las normas de conflicto de los Estados Miembros de la Unión Europea materialmente orientadas a la protección del titular del Derecho a la Protección de Datos en el marco de una transferencia internacional de datos de carácter personal ilícita", en *Revista Mexicana de Derecho Internacional Privado y Comparado*, N.º 48, Academia Mexicana de Derecho Internacional Privado y Comparado, México, octubre 2022, Disponible en: www.amedip.org, pp. 13-30.

ORTEGA GIMÉNEZ, A., "Schrems II" y las transferencias internacionales de datos personales UE-EE.UU., en TOMÁS MALLÉN, B.; GARCÍA MAHAMUT, R., PAUNER CHULVI, C. (Edit.) y VIGURI CORDERO, J.A. (Coord.), *Las cláusulas específicas del Reglamento General de Protección de Datos en el ordenamiento jurídico español. Cuestiones clave de orden nacional y europeo*, Editorial Tirant lo Blanch, Valencia 2021, pp. 91-117.

ORTEGA GIMÉNEZ, A., "Sanciones sobre transferencias internacionales de datos", en DAVARA FERNNADEZ DE MARCOS, E. y DAVARA FERNANDEZ DE MARCOS, L. (Coords.), *Análisis práctico de sanciones en materia de Protección de Datos -Divididas por conceptos y sectores-*, Editorial Thomson Reuters Aranzadi, Cizur Menor (Navarra), 2021, pp. 613-635.

ORTEGA GIMÉNEZ, A., "COVID-19: Un desafío para la protección de datos de carácter personal" en ORTEGA GIMÉNEZ, A. (Dir.); HEREDIA SÁNCHEZ, L.; y LORENTE MARTÍNEZ, I. (Coords.), *Problemas que el COVID-19 plantea en el trinomio protección de datos, transferencia y movilidad. Aportación de soluciones prácticas desde la ciencia jurídica*, Editorial Thomson Reuters Aranzadi, Cizur Menor (Navarra), abril 2021, pp. 15-21.

ORTEGA GIMÉNEZ, A., "Decisiones relativas a las cláusulas contractuales tipo para las transferencias internacionales de datos personales a terceros países y entre los responsables y encargados del tratamiento", *Revista LA LEY Privacidad*, número 9, Editorial Wolters Kluwer, Madrid, julio-septiembre 2021, pp. 1-12.

ORTEGA GIMÉNEZ, A., "Autoridades de control de un Estado miembro y tratamiento transfronterizo de datos, tras la STJUE de 15 de junio de 2021 (Asunto C-645/19)", en *Revista LA LEY Privacidad*, número 9, Editorial Wolters Kluwer, Madrid, julio-septiembre 2021, pp. 1-12.

ORTEGA GIMÉNEZ, A., "Brexit, international private relations and personal data protection, after the new association agreement EU-United Kingdom", en *International Journal of Law, Policy and Social Riew*, volumen 3, Cambridge university press, Reino Unido, 03 de marzo de 2021, pp. 19-27.

ORTEGA GIMÉNEZ, A. y GARCÍA ESCOBAR, E., "Réquiem por el Escudo de Privacidad (tras la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 "Schrems II")", en *Revista Aranzadi Unión Europea*, número 11, Editorial Aranzadi, S.A.U., Cizur Menor (Navarra), 02 de marzo de 2021, PP.RR.-5.10.

ORTEGA GIMÉNEZ, A., "Tratamiento ilícito internacional de datos personales, reglamento general de protección de datos y derecho internacional privado: cuestiones de

competencia judicial internacional y de determinación de la ley aplicable", Parte 3 – Capítulo I, La protección de datos en la era digital, en FUENTES SORIANO, O. (Directora); ARRABAL PLATERO, P.; DOIG DÍAZ, Y.; ORTEGA GIMÉNEZ, A.; TURÉGANO MANSILLA, I. (Coordinadores), *Era Digital, Sociedad y Derecho*, Tirant lo Blanch, Valencia, 2020, pp. 521-545.

ORTEGA GIMÉNEZ, A., "Hacia la "libre circulación de datos de carácter personal": el nuevo Reglamento General de Protección de Datos de la UE", *Estudios sobre la Jurisprudencia Europea. Materiales del III Encuentro anual del Centro español European Law Institute*, volumen II, Editorial Jurídica Sepin, Madrid, 2020, pp. 1065-1075.

ORTEGA GIMÉNEZ, A. y GARCÍA ESCOBAR, E., "Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 ("Schrems II")", en *LA LEY Privacidad*, número 6, Editorial Wolters Kluwer, Madrid, octubre-diciembre 2020, pp. 1-22.

ORTEGA GIMÉNEZ, A., "Tratamiento ilícito internacional de datos personales, Reglamento General de protección de datos y derecho internacional privado: cuestiones de competencia judicial internacional y de determinación de la ley aplicable", en *Revista CEFLegal, Centro de Estudios Financieros*, Madrid, agosto-septiembre 2020, pp. 53-80.

ORTEGA GIMÉNEZ, A., "Tutela jurisdiccional ante un tratamiento ilícito internacional de datos personales y el nuevo Reglamento General de Protección de Datos de la Unión Europea", en *Revista Acta Judicial*, número 6, Ilustre Colegio Nacional de Letrados de la Administración de Justicia, Madrid, julio 2020, pp. 02-23.

RALLO LOMBARTE, A. y GARCÍA MAHAMUT, R., *Hacia un nuevo Derecho europeo de protección de datos*, Tirant lo blanch, Valencia, 2015.

SANCHO VILLA, D., *Negocios internacionales de tratamiento de datos personales*, Navarra, Civitas, 2010.

SANCHO VILLA, D., *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003.