Trabajo Fin de Grado

Las transferencias de datos internacionales en el Derecho de la Unión Europea. Situación actual y perspectivas de futuro.

International data transfers under European Union Law. The current situation and future perspectives.

Autor/es

Javier Blasco Aso

Director/es

Ana Gascón Marcén

Facultad de Derecho

Curso 2021/2022

ÍNDICE:

I. INTRODUCCIÓN 4
1. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS 4
2. JUSTIFICACIÓN. 4
3. METODOLOGÍA 5
II. DERECHO DE PROTECCIÓN DE DATOS PERSONALES 6
1. INTRODUCCIÓN 6
2. MARCO LEGAL DEL DERECHO DE PROTECCIÓN DE DATOS. 7
2.1 De la Directiva al Reglamento General sobre Protección de Datos. 7
2.2 Otras normas de aplicación 8
III. LA LIBRE CIRCULACIÓN DE DATOS PERSONALES 9
1. TRANSFERENCIAS DE DATOS PERSONALES DENTRO DEL ESPACIO ECONÓMICO EUROPEO 10
2. TRANSFERENCIAS INTERNACIONALES DE DATOS. 10
2.1. Transferencias basadas en una decisión de adecuación 11
2.2. Transferencias mediante garantías adecuadas. 15
2.3. Normas corporativas vinculantes o Binding Corporate Rules. 18
2.4. Transferencias basadas en acuerdos internacionales 19
2.5. Excepciones para situaciones específicas. 19
2.6. El caso de Estados Unidos. 21
IV. LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES: REGLAMENTO 2018/1807, RELATIVO A UN MARCO PARA LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES EN LA UNIÓN EUROPEA 27
V. UNA ESTRATEGIA EUROPEA DE DATOS. ESPECIAL MENCIÓN A LA PROPUESTA DE REGLAMENTO RELATIVO A LA GOBERNANZA EUROPEA DE DATOS. 29
1. LA ESTRATEGIA. 31
2. SITUACIÓN ACTUAL 40
VI. CONCLUSIONES 42
VII. BIBLIOGRAFÍA 43
1. ARTÍCULOS, CAPÍTULOS DE LIBROS Y ENTRADAS DE BLOG 43
2. FUENTES INSTITUCIONALES 45

Listado de abreviaturas:

AEPD: Agencia Española de Protección de Datos.

CDFUE: Carta de los Derechos Fundamentales de la Unión Europea

CE: Comisión Europea.

CEPD: Comité Europeo de Protección de Datos.

DOUE: Diario Oficial de la Unión Europea.

EEE: Espacio Económico Europeo.

GT 29: Grupo de Trabajo del art. 29.

LGD: Ley de Gobernanza de Datos.

LMD: Ley de Mercados Digitales.

LOPDGDD: Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales en España.

LSD: Ley de Servicios Digitales.

BCRs: Normas Corporativas Vinculates *(Blinding Corporate Rules)*.

RGPD: Reglamento General de Protección de Datos.

RIA: Reglamento sobre un enfoque europeo en materia de inteligencia artificial

SCCs: Cláusulas contractuales tipo.

SEPD: Supervisor Europeo de Protección de Datos.

SWIFT: Sociedad de las Telecomunicaciones Financieras Interbancarias Mundiales.

TFUE: Tratado de Funcionamiento de la Unión Europea.

TUE: Tratado de la Unión Europea.

TJUE: Tribunal de Justicia de la Unión Europea.

UE: Unión Europea.

I. INTRODUCCIÓN

1. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

El presente Trabajo de Fin de Grado tiene por objeto establecer un análisis de la regulación a nivel de la Unión Europea del Derecho de la Protección de Datos. En especial, se pone el foco en las transferencias internacionales de datos, los mecanismos para realizarlas y los instrumentos surgidos en torno a ellas. De esta forma, conviene distinguir el régimen previsto en el ámbito del Reglamento General de Protección de Datos (RGPD)[1] para aquellas transferencias de datos personales, del marco legal existente para las que no tienen tal carácter.

En el trabajo se va a hacer hincapié en los mecanismos jurídicos previstos en el RGPD para la realización de las transferencias internacionales de datos y en los problemas surgidos con EE.UU. en relación con las Sentencias del Tribunal de Justicia de la Unión Europea *Schrems I* y *Schrems II*, así como las soluciones que se han planteado para solventar la situación.

Para finalizar, se analizará la estrategia que la Comisión Europea ha planteado para los próximos años con el objeto de situar a la UE como una de las grandes potencias en el almacenamiento y tratamiento de datos.

2. JUSTIFICACIÓN.

En los últimos años, los flujos de datos están creciendo exponencialmente debido al desarrollo de las tecnologías de la información y de la comunicación que han transformado nuestra economía y sociedad. Todo ello ha permitido un rápido crecimiento de la cantidad de datos en circulación y ha puesto sobre la mesa nuevos problemas y retos a los que hacer frente desde muy diversos ámbitos. Al mismo tiempo, la globalización ha difuminado las fronteras entre los Estados, dificultando el control de los movimientos de información por parte de los mismos y permitiendo el acceso a datos sin grandes restricciones.

En este contexto, surge la exigencia de establecer un marco jurídico que regule la materia y garantice un nivel de protección de datos suficiente. Dado el carácter global del

[1] RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

fenómeno, la protección a nivel estatal resulta insuficiente y es por ello, por lo que surge la necesidad de trabajar a nivel supranacional logrando una adecuada cooperación en la materia.

Como posteriormente se analizará, la protección de datos ha sido objeto de regulación a nivel internacional por medio del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981 (Convenio nº 108).

En el ámbito de la Unión Europea, y en el marco de un mercado único, también se ha puesto de manifiesto la necesidad de regular este fenómeno. Así, en la actualidad se dispone de un sólido ámbito de protección de los datos de carácter personal, destacando el Reglamento General de Protección de Datos (RGPD). Por otro lado, de forma más reciente, se ha puesto de manifiesto la necesidad de crear un marco legal que regule los datos de carácter no personal debido al crucial papel que están desempeñando en el ámbito de la investigación, la innovación y el desarrollo económico y que también será analizado a lo largo del trabajo.

En el mundo interconectado en el que nos encontramos, cobran especial importancia las transferencias internacionales de datos. Así, como ya se ha indicado, el objeto del presente trabajo va a ser analizar el régimen legal existente en el ámbito de la UE, distinguiendo las transferencias realizadas dentro del mercado interior donde no opera ninguna limitación, y las transferencias que se producen hacia terceros Estados y los mecanismos normativos que se han previsto y la problemática surgida en torno a ellos.

Para finalizar, resulta necesario hacer referencia a las perspectivas de futuro y el marco planteado por la Comisión a través de una serie de propuestas normativas en el ámbito de los servicios y mercados digitales, la gobernanza de datos y la regulación de la inteligencia artificial. Además, en el primer semestre del año 2022 se presentó la propuesta de Ley de Datos.

3. METODOLOGÍA

Se comenzará realizando un estudio cualitativo con metodología deductiva sobre la situación de la regulación en la materia y las perspectivas de las instituciones de cara al futuro, planteando una serie de críticas y conclusiones basadas en la coherencia, mejora y garantía de la regulación de las Transferencias Internacionales de Datos respecto del marco común de protección de los mismos.

De esta forma, se va a proceder a través del análisis descriptivo, literario, histórico y jurídico, primando el marco legal vigente, así como las propuestas normativas planteadas por la Comisión. También tienen un papel importante las Comunicaciones de la Comisión Europea, así como las declaraciones de órganos europeos como es el caso del Comité Europeo de Protección de Datos (CEPD).

Asimismo, se ha analizado la literatura científica en la materia, tanto a nivel nacional como internacional, que incluye un amplio estudio sobre la disciplina y los sucesos y novedades que han ido aconteciendo. Por último, no hay que olvidar la labor realizada por el TJUE a raíz de las dos principales sentencias que nos afectan: Schrems I[2] y Schrems II[3].

II. DERECHO DE PROTECCIÓN DE DATOS PERSONALES

1. INTRODUCCIÓN

El Derecho a la protección de datos personales se encuentra consagrado en el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea, así como en el art. 16.1 del Tratado de Funcionamiento de la Unión Europea (TFUE).

En el caso de la Carta, se reconoce el derecho de toda persona a la protección de datos de carácter personal y se establece que el tratamiento se realizará de "modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley". Continúa el precepto en cuestión reconociendo el derecho de acceso a los datos recogidos que le conciernan, junto con el derecho de rectificación. Para finalizar, se sujeta la materia al control por una autoridad independiente. De esta forma, se trata de una novedad recogida en la normativa actual, si bien con anterioridad, el TEDH[4] ya lo había considerado en la jurisprudencia como parte del contenido del Derecho a la privacidad[5].

---

[2] Sentencia del TJUE de 6 de octubre de 2015, asunto C-362/14, Maximiallian Schrems v. Commissioner (Caso Schrems). ECLI:EU:C:2015:650.

[3] Sentencia del TJUE de 16 de julio de 2020, asunto C-311/18 Data Protection Commissioner v. Facebook Ireland Limited y Maximillian Schrems (Caso Schrems II) ECLI:EU:C:2020:59.

[4] El Tribunal Europeo de Derechos Humanos es el órgano jurisprudencial encargado del control de la aplicación del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales por sus Estados parte. A pesar de tratarse de un acuerdo internacional del que la UE no es parte, el art. 6.3 del TUE incluye como principios generales que forman parte del Derecho de la Unión los derechos fundamentales que garantiza el Convenio.

[5] Martín y Pérez de Nanclares, J. (2008) Comentario al artículo 8: Protección de Datos de Carácter Personal. *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo.* Fundación BBVA, 223-243 (Pág. 237). https://www.fbbva.es/wp-

Por otro lado, en relación con el art. 16.1 TFUE, se ha proclamado en similares términos el reconocimiento del derecho a la protección de datos. Asimismo, se establece un mandato al Parlamento Europeo y al Consejo para que a través del procedimiento legislativo ordinario desarrollen las normas sobre protección de las personas físicas en relación con el tratamiento de sus datos en el ámbito de aplicación del Derecho de la Unión, así como en relación con la libre circulación de los mismos.

2. MARCO LEGAL DEL DERECHO DE PROTECCIÓN DE DATOS.

2.1 De la Directiva al Reglamento General sobre Protección de Datos.

En el ámbito de la Unión Europea, la materia había sido regulada por medio de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En este sentido, la Directiva surgió en un contexto en el que varios Estados miembros ya habían adoptado leyes nacionales de protección de datos. Consecuentemente, tenía por objeto la armonización de las regulaciones nacionales para garantizar la protección de los datos personales, así como la libre circulación de los mismos entre todos los Estados miembros.

De esta forma, se estableció un detallado marco de protección de datos en la Unión Europea. No obstante, dado el margen de discrecionalidad en la transposición de la norma, esta se incorporó a los diferentes Estados de forma desarmonizada.

En este marco, finalmente, en el año 2016 se produjo la aprobación del Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (RGPD). No obstante, de acuerdo con el art. 99 RGPD, a pesar de entrar en vigor en el año 2016, no fue aplicable hasta el 25 de mayo de 2018.

La aprobación del Reglamento General de Protección de Datos produjo la unificación y modernización de la legislación de la Unión Europea en la materia, así como la adecuación de la misma a la protección de los derechos fundamentales en el contexto económico y digital en el que nos encontramos.

---

content/uploads/2017/05/dat/DE_2008_carta_drechos_fundamentales.pdf (Consultado a 5 de junio de 2022).

El Reglamento contiene 11 Capítulos que desarrollan las disposiciones generales, proclaman una serie de principios en la materia, así como los Derechos de las personas físicas. Por otro lado, se regulan las figuras del responsable del tratamiento y del encargado del tratamiento y en el Capítulo V se regulan las transferencias de datos personales a terceros países u organizaciones internacionales. A continuación, se establece el marco legal de las autoridades de control independientes y la parte final del Reglamento se reserva a la cooperación, recursos, responsabilidad y sanciones, situaciones específicas, actos delegados y de ejecución, junto con disposiciones finales. En general, las principales disposiciones vinculan a las organizaciones a aplicar la protección de los datos desde el diseño y por defecto, la designación de un delegado de protección de datos cuando proceda, al respeto al derecho a la portabilidad de los datos y al principio de responsabilidad proactiva.

Desde su aprobación, los Estados miembros han venido modificando sus legislaciones nacionales en la materia, como es el caso de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en España (LOPDGDD).

2.2 Otras normas de aplicación

Asimismo, en el ámbito de la Unión Europea hay que hacer referencia a otros instrumentos que, si bien de forma más específica, han desarrollado la regulación de ciertos aspectos del Derecho a la protección de datos personales.

De esta forma, en primer lugar hay que hacer mención a la Directiva 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Por otro lado, en relación con las comunicaciones electrónicas se aprobó la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Así, la Directiva sobre la privacidad y las comunicaciones electrónicas establece normas sobre el tratamiento de los datos personales y la protección

de la intimidad en el ámbito de dichas comunicaciones, desarrollando disposiciones sobre la seguridad de los datos personales en redes, la notificación de violaciones de los datos personales y la confidencialidad de las comunicaciones[6].

Asimismo, hay que destacar la labor llevada a cabo por el Tribunal de Justicia de la Unión Europea. Desde la aprobación de la Directiva sobre protección de datos personales se ha ido desarrollando una importante base jurisprudencial que aclara el alcance y significado de los principios de protección de datos y del derecho a la protección de datos personales[7].

III. LA LIBRE CIRCULACIÓN DE DATOS PERSONALES

En primer lugar, resulta necesario acotar la materia, pues, como ya se indicó en la introducción, hay que distinguir el régimen previsto para los datos personales de los que no tienen tal carácter. Así, el art. 4.1 RGPD estipula que se entiende por dato personal "toda información sobre una persona física identificada o identificable".

De tal forma que aquellos datos relacionados con una persona física identificada o identificable, se regirán por las previsiones establecidas por el RGPD. Por el contrario, aquellos datos que no tengan el carácter de personales quedarán fuera del ámbito de aplicación de la norma.

Por lo tanto, se trata de una cuestión de gran relevancia. En este sentido, en relación con la libre circulación de los datos no personales, establece el Reglamento (UE) 2018/1807 que tienen la consideración de datos no personales los que no tengan el carácter de personales de acuerdo con el RGPD.

De esta forma, es necesario hacer hincapié en que las cuestiones relativas a la libre circulación y a las transferencias internacionales de datos personales se regirán por las previsiones del RGPD, mientras que en materia de transferencias de datos de carácter no personal rige el Reglamento (UE) 2018/1807.

---

[6] En este sentido, la Comisión lleva años persiguiendo la modernización de la regulación actual a través de un reglamento que vaya en línea con el RGPD. De esta forma se planteó la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), si bien, debido a la falta de acuerdo entre el Parlamento y el Consejo, por el momento, no ha salido adelante.

[7] Tribunal de Justicia de la Unión Europea: *Ficha Temática: Protección de los Datos de Carácter Personal*, Dirección de Investigación y Documentación. (julio de 2018). https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_es.pdf (Consultado a 5 de junio de 2022).

Una vez analizado el ámbito de aplicación objetivo del RGPD, es necesario distinguir entre: a) libre circulación de datos personales gestionados en el mercado interior; b) transferencias transfronterizas de datos; c) transferencias internacionales de datos.

1. TRANSFERENCIAS DE DATOS PERSONALES DENTRO DEL ESPACIO ECONÓMICO EUROPEO

Comienza el artículo 1.3 RGPD indicando que la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Asimismo, todo ello hay que enmarcarlo dentro de la Decisión del Consejo y de la Comisión de 13 de diciembre de 1993, relativa a la celebración del acuerdo sobre el EEE. De esta forma, el ámbito de la libre circulación de datos personales abarca también a los Estados miembros del EEE. Por lo tanto, además, de los países pertenecientes a la UE, hay que incluir también a Islandia, Liechtenstein y Noruega.

En cuanto a las transferencias de datos transfronterizas, se trata de movimientos de datos de carácter personal entre agencias de controladores o procesadores de datos de múltiples Estados miembros, así como las transferencias de datos personales de partes interesadas en múltiples Estados miembros dentro de un único Estado miembro de la UE que establece controladores o procesadores.

2. TRANSFERENCIAS INTERNACIONALES DE DATOS

Se trata de las transmisiones de datos que han sido objeto de mayor debate. A pesar de la transcendencia que tienen en la práctica jurídica, el RGPD no ha definido el concepto de transferencia internacional de datos. No obstante, éste ha sido acotado por la Agencia Española de Protección de Datos (AEPD) quien las define como aquellas que suponen un flujo de datos personales desde el territorio nacional a destinatarios establecidos fuera de países del EEE.

Como ya se ha comentado, una de las principales aportaciones del RGPD fue dotar al marco normativo de la UE en materia de protección de datos de un alcance general y armonizar las legislaciones de todos los Estados miembros. A ello hay que añadir, en

materia de transmisiones internacionales de datos personales y dentro del ámbito nacional, el Título VI de la LOPDGDD[8].

En la primera aproximación al tema de la regulación a través del RGPD, es necesario resaltar lo dispuesto en los Considerandos del Reglamento. En primer lugar, el número 6, debido a los nuevos desarrollos tecnológicos, hace referencia a la necesidad de "facilitar aún más la libre circulación de datos personales dentro de la Unión y su transferencia a terceros países y organizaciones internacionales, asegurando un alto nivel de protección de los datos personales". Mientras que el considerando 13 indica la necesidad de garantizar la seguridad jurídica y la transparencia para el libre flujo de datos personales en el mercado interior.

En cuanto al régimen jurídico, las transferencias internacionales de datos se rigen por el marco establecido en el Capítulo V del RGPD. Por lo tanto, requieren uno de los siguientes mecanismos:

1. Transferencias basadas en una decisión de adecuación.
2. Transferencias mediante garantías adecuadas.
3. Normas Corporativas Vinculantes o Binding Corporate Rules.
4. Transferencias basadas en acuerdos internacionales

A continuación, se va a proceder al análisis pormenorizado de las mismas.

2.1. Transferencias basadas en una decisión de adecuación

Indica el art. 45.1 RGPD que: "Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado".

De esta forma, el órgano competente para dictar la decisión de adecuación es la Comisión Europea. Para ello, debe analizar y evaluar el grado de protección de datos personales del país que corresponda a través de los elementos enumerados en el apartado segundo del artículo.

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en España.

No obstante, como bien ha anotado Cordero[9], el alcance de las decisiones de adecuación de la Comisión no es absoluto, pues se trata de una presunción *iuris tantum* de que existe un nivel adecuado de garantías tal y como consideró el TJUE en la Sentencia Schrems I[10]. De tal forma que este tipo de actos no impiden a las autoridades nacionales de control el ejercicio de sus facultades en el ámbito de la protección de datos de conformidad con los arts. 7, 8 y 47 CDFUE.

Así, las sentencias del TJUE declarando contrarios a derecho los acuerdos entre EE.UU. y la UE para posibilitar las transferencias internacionales de datos personales y que se analizarán en detalle posteriormente son un claro ejemplo de la falta de alcance absoluto de los actos de la Comisión.

En cuanto a los requisitos a los que hace referencia el art. 45.2 RGPD que deberán ser evaluados, se pueden sintetizar de la siguiente forma:

- El estado de Derecho, el respeto de los Derechos Humanos y las Libertades Fundamentales, la legislación pertinente, el acceso de las autoridades públicas a los datos personales, la aplicación de la legislación en la materia, las normas de protección de datos, las normas profesionales y las medidas de seguridad, la jurisprudencia, entre otros.
- La existencia y el funcionamiento efectivo de autoridad/es de control independiente en el tercer país o a las cuales esté sujeta una organización internacional.
- Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes.

Asimismo, a través de la Comunicación al Parlamento Europeo y al Consejo relativa al Intercambio y Protección de los datos personales en un mundo globalizado[11], la Comisión ha planteado una serie de "prerrequisitos" para la decisión de adecuación. De tal forma que se incluyen los siguientes:

[9] Cordero Álvarez, C. I. (2019). La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la Cloud Act. *Revista Española de Derecho Europeo*, (70), 49-108, p. 75.
[10] Sentencia del TJUE de 6 de octubre de 2015, asunto C-362/14, Maximiallian Schrems v. Commissioner (Caso Schrems). ECLI:EU:C:2015:650. Ap. 73, 74 y 96.
[11] Comunicación (COM(2017) 7 final) de la Comisión al Parlamento Europeo y al Consejo relativa al Intercambio y Protección de los datos personales en un mundo globalizado.

1. El alcance de las relaciones comerciales —efectivas o posibles— con el tercer país.
2. La magnitud de los flujos de datos personales con origen en la UE.
3. Si el tercer país es pionero en el ámbito de la protección de datos y la privacidad y puede servir de modelo para otros países de su región.
4. La relación política global con el tercer país en cuestión, en particular por lo que respecta al fomento de valores comunes y objetivos compartidos a escala internacional.

Como indica Juan José Gonzalo Domenech[12], cualquier análisis significativo de la protección adecuada debe comprender tanto el contenido de las normas aplicables como los medios para garantizar su aplicación efectiva. Es por ello, por lo que la Comisión Europea deberá verificar de forma periódica que las normas establecidas sean efectivas en la práctica.

Este modelo a seguir parte de la propia Carta de los Derechos Fundamentales de la Unión Europea, el RGPD, junto con los convenios y estándares internacionales de aplicación.

En este sentido, el Grupo de Trabajo sobre Protección de Datos creado en virtud del art. 29 de la Directiva 95/46/CE, como órgano consultivo independiente de la UE, ha planteado por medio del Documento de Trabajo[13] (WP 254) de Referencias sobre adecuación los principios generales para garantizar un nivel equivalente de protección de datos en un tercer país, territorio, sectores u organizaciones internacionales. Para ello, se pone de relieve que el sistema del tercer país u organización internacional incluya similares conceptos, bases legales, principios, derechos y restricciones que el marco de protección de datos previsto en el RGPD.

Respecto a quien puede instar el procedimiento para la toma de una decisión de adecuación, en cualquier caso, puede ser por la propia Comisión, así como el Comité Europeo de Protección de Datos (art. 70.1.s); igualmente, por un Acuerdo Internacional suscrito por la Comisión, como fue el caso para Estados Unidos en el año 2016 o con

[12] Gonzalo Domenech, J. J. (2019). Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros. *Cuadernos de Derecho Transnacional*, (Marzo 2019) Vol. 11, Nº 1, p. 357. https://doi.org/10.20318/cdt.2019.4624 (Consultado a 5 de junio de 2022).

[13] Grupo de Trabajo del Artículo 29: Documento de Trabajo sobre Referencias de Adecuación (WP254). Revisado 6 de febrero de 2018. https://ec.europa.eu/newsroom/article29/items/614108 (Consultado a 5 de junio de 2022).

Japón; y, para finalizar, el propio interesado, siempre que cumpla con los requisitos previos exigidos puede instar una decisión de adecuación.

Posteriormente, la Comisión valorará el cumplimiento de los requisitos enunciados y emitirá una Decisión de Adecuación del tercer país, territorio, sector u organización internacional relativa a la existencia de un nivel de protección adecuado. De esta forma, la decisión constituye un acto ejecutivo, tal y como dispone el apartado tercero del artículo 45 RGPD.

No obstante, hay que añadir la existencia de un sistema de control para la Decisión de Adecuación. En este ámbito, hay que hacer referencia al Reglamento 182/2011, del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión. En el marco del citado Reglamento, se requerirá que el proyecto sea sometido al dictamen de un comité de representantes de los miembros de la UE. Hay que destacar que el dictamen tiene carácter vinculante.

Por otro lado, de acuerdo con el art. 70.1.s) RGPD y con carácter previo a la decisión final de la CE, se faculta al CEPD para que dictamine sobre la adecuación del tercer Estado, región u organización internacional.

Para finalizar, establece el apartado tercero del art. 45 RGPD que: "El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional". De esta forma, en el caso de que no se cumpliera el nivel de adecuación exigido, la Comisión podrá derogar, suspender o modificar la decisión. No obstante, como bien prevé el art. 45.6 RGPD, las partes iniciarán negociaciones para poner remedio a la situación de prohibición de las transferencias internacionales en el marco de las decisiones de adecuación derogadas o suspendidas.

Asimismo, es necesario hacer mención a que las decisiones de adecuación realizadas por la Comisión Europea en el marco de la Directiva 95/46/CE mantienen su vigencia en tanto no sean modificadas, sustituidas o derogadas por una Decisión posterior llevada a cabo por la Comisión.

En la actualidad, los terceros países los que se les ha reconocido un nivel de adecuación similar son Suiza, Canadá, Corea del Sur, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Japón y Reino Unido[14].

2.2. Transferencias mediante garantías adecuadas

Esta posibilidad se encuentra prevista en el art. 46 RGPD. En este sentido, se prevé en su apartado primero, que en el caso de inexistencia de la decisión de adecuación a la que hace referencia el art. 45.3 RGPD, solo podrán transferirse los datos de carácter personal a un tercer Estado u organización internacional si hubiere ofrecido garantías adecuadas y se disponga para los interesados de la garantía de sus derechos exigibles y acciones legales efectivas.

De tal forma que estamos ante una norma supletoria para aquellas situaciones en las que la CE no haya emitido un acto ejecución determinando sobre la existencia de un nivel de protección adecuado.

Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el

[14] *Adequacy decisions*. (2017, noviembre 4). Comisión Europea - European Commission. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_es (Consultado a 5 de junio de 2022). Respecto a las decisiones relativas a Estados Unidos, serán analizadas en el apartado 3.6.

tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

De esta forma, la concurrencia de alguna de las citadas circunstancias da lugar a una presunción *iuris tantum*[15] de que la transferencia cuenta con unas garantías equivalentes a las exigidas dentro del EEE.

Por otro lado, a raíz de la Sentencia Schrems I[16], el TJUE consideró que la CE no es competente para limitar el ámbito de poder y actuaciones de las autoridades de control nacionales. Por lo tanto, la CE no puede impedir que estas autoridades ejerzan sus funciones, incluido la suspensión o prohibición de realización de transferencias de datos internacionales, cuando sean contrarias a la normativa en materia de protección de datos, tanto nacional, como de la UE.

Como posteriormente se analizará a raíz de la Sentencia Schrems II[17], las cláusulas tipo (SCCs) son el mecanismo más utilizado para las transferencias internacionales[18]. Además, como consecuencia de la citada Sentencia y de la entrada en aplicación del RGPD, la Comisión adoptó unas nuevas cláusulas tipo que vienen a sustituir a las establecidas anteriormente.[19]

Además, con Schrems II el uso de las SCCs resulta más complejo debido a la necesidad de realizar una evaluación previa. De esta forma, las nuevas cláusulas se adaptan al RGPD incorporando los principios de responsabilidad proactiva y tratan de adoptar los criterios señalados por el TJUE en la sentencia del caso Schrems II. No obstante, sigue siendo necesario que el exportador de los datos, en su caso ayudado por el importador, analice el impacto que la legislación y/o la práctica vigente en el país del importador pueda tener en el nivel de protección proporcionado, de forma que sea esencialmente equivalente al que proporciona el marco europeo.

---

[15] Cordero Álvarez C. op. cit. p. 76.
[16] Schrems I op. cit.
[17] Schrems II op. cit.
[18] *IAPP-EY annual Privacy Governance Report 2021*. (s/f). Iapp.org. Recuperado el 14 de mayo de 2022. https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf (Consultado a 5 de junio de 2022).
[19] Decisión de Ejecución (UE) 2021/914 de la Comisión de 4 de junio de 2021 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

Además, adicionalmente, deberán tenerse en cuenta las directrices del CEPD[20] sobre las medidas suplementarias que se considere adecuado adoptar para garantizar ese nivel de protección equivalente[21]. Así, para aplicar el principio de responsabilidad proactiva a las transferencias de datos plantea una guía de actuación que se basa en el conocimiento de las transferencias, la determinación de los instrumentos en los que se fundamentan y la evaluación del instrumento del art. 46 RGPD que resulte más eficaz, junto con la adopción de medidas complementarias eficaces y la reevaluación a intervalos adecuados.

En relación, con las medidas complementarias, resulta destacable el Anexo 2 de las directrices donde se plantean una serie de medidas técnicas, contractuales y organizativas para llevar a cabo.

Asimismo, de acuerdo con el artículo 46.3.a) RGPD, además de las cláusulas tipo formuladas por la CE, nada impide a los responsables la formulación de otro tipo de cláusulas contractuales siempre y cuando estas sean aprobadas por la correspondiente autoridad de control. Para ello, de acuerdo con lo estipulado en el apartado cuarto del citado precepto, las autoridades competentes deberán aplicar el mecanismo de coherencia a que hace referencia el art. 63 y 64 RGPD, y, por lo tanto, el Comité Europeo de Protección de Datos emitirá un dictamen sobre la materia que deberá ser tenido en cuenta, en la medida de lo posible, en la toma de la decisión.

Entre las demás garantías, también se prevén las cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la CE, siendo similares a las ya enunciadas y en este caso, requiriendo una vez han sido adoptadas por la correspondiente autoridad, la aprobación por la CE.

En cuanto a los Códigos de conducta, de acuerdo con el art. 40.1 RGPD, tienen por objeto la correcta aplicación del Reglamento y podrán ser promovidos por los Estados miembros, autoridades de control, el Comité y la Comisión.

---

[20] Recomendaciones del CEPD de 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE Adoptadas el 10 de noviembre de 2020 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf (Consultado a 5 de junio de 2022).

[21] Christakis, T. (2020) "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers. *European Law Blog.* https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/ (Consultado a 5 de junio de 2022).

Asimismo, los mecanismos de certificación que de conformidad con el art. 42 RGPD serán promovidos por los Estados miembros, autoridades de control, el Comité y la Comisión con el objeto de demostrar el cumplimiento de lo dispuesto en el Reglamento en el marco de las operaciones de tratamiento de los responsables y encargados.

Por otro lado, el art. 46.3.b) RGPD hace referencia a disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. Por lo que en este caso, al igual que ocurría con las cláusulas tipo contractuales, previa autorización de la autoridad de control competente, podrán ser aportadas las garantías adecuadas de este modo.

No obstante, aquí hay que hacer mención al art. 42.1 LOPDGDD al establecer que "Las transferencias internacionales de datos (…) 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 anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos".

2.3. Normas corporativas vinculantes o Binding Corporate Rules

Se prevé en el art. 47 RGPD la aprobación de Normas Corporativas Vinculantes o *Blinding Corporate Rules (BCRs)* por parte de la autoridad competente que permitan a grupos de empresas, así como a uniones de empresas, la realización de transferencias internacionales. De esta forma, se han definido por el GT 29 como "códigos de conducta que redactan y siguen organizaciones multinacionales que contienen medidas internas pensadas para poner en práctica principios de protección de datos". Por lo tanto, la autoridad competente en el Estado miembro podrá aprobar las Normas Corporativas Vinculantes siempre que cumplan con los requisitos exigidos por la normativa y siempre de acuerdo con el mecanismo de coherencia (arts. 63 y 64.1.f) RGPD).

En cuanto a los requisitos de estas formas, tal y como indica el apartado primero del art. 47, estas deberán: a) ser jurídicamente vinculantes y de cumplimiento por todos los miembros del grupo empresarial o de la unión de empresas en cuestión; b) conferir expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales; y c) cumplir los requisitos enunciados en el apartado segundo.

Respecto a estos requisitos, el apartado segundo, establece una serie de elementos que deberán especificar las Normas Corporativas Vinculantes. Así, de forma ejemplificativa,

hay que referirse a la estructura y los datos de contacto del grupo o unión de empresas; las trasferencias y el tipo de tratamiento, así como sus fines; la aplicación de los principios generales en materia de protección de datos; los derechos de los interesados y los medios para ejercerlos; o los procedimientos de reclamación, entre otros.

Para finalizar, hay que hacer mención a que la primera Norma Corporativa Vinculante en Europa desde que comenzó a aplicarse el RGPD fue para el Grupo Fujikura Automotive Europe y que fue autorizada por la Agencia Española de Protección de Datos en el año 2020.

2.4. Transferencias basadas en acuerdos internacionales

Tal y como estipula el Considerando nº 102 del RGPD, la UE puede celebrar acuerdos internacionales con terceros países que regulen la transferencia de datos personales con fines concretos. Asimismo, se reconoce la posibilidad a los Estados miembros para celebrar acuerdos internacionales que impliquen "la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al RGPD ni al Derecho de la Unión e incluyan un nivel adecuado de protección de los Derechos Fundamentales de los interesados".

En este ámbito se pueden citar como ejemplos los acuerdos relativos a Registros de nombres de pasajeros. Así, se han alcanzado acuerdos para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo o delitos graves transnacionales con EE.UU., Australia y Canadá. Por otro lado, se adoptó en 2016 la Directiva (UE) 2016/861 (Directiva PNR) que establece el marco jurídico para la transferencia de este tipo de datos a terceros países.

Mención especial requiere la Sociedad de las Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) que lleva a cabo el tratamiento de prácticamente la totalidad de transferencias monetarias mundiales desde bancos europeos. Tras un intenso debate con EE.UU. se llegó a lo que se conoce como Acuerdo Swift que permite al Departamento del Tesoro de los Estados Unidos acceder a los datos financieros almacenados por SWIFT siempre y cuando se autorice por EUROPOL y se identifiquen los datos requeridos en una solicitud motivada, no se pida ningún dato sobre la zona única de pagos en euros y se limite a los datos estrictamente necesarios.

2.5. Excepciones para situaciones específicas

El art. 49 RGPD dispone que en ausencia de una decisión de adecuación (art. 45 RGPD) o de garantías adecuadas (art. 46 RGPD), incluidas las normas corporativas vinculantes, una transferencia o conjunto de transferencias de datos personales a un tercer país u organización internacional solo podrá realizarse si se cumple alguna de las condiciones que enumera. De esta forma, el apartado primero enumera las siguientes condiciones:

1. El interesado haya dado explícitamente su consentimiento a la transferencia propuesta, siendo informado de los posibles riesgos debido a la ausencia de decisión de adecuación y de garantías adecuadas.
2. La transferencia sea necesaria para la celebración o ejecución de un contrato por el interesado o en su propio interés, así como medidas precontractuales, en su caso.
3. La necesidad de la transferencia por razón de interés público.
4. La necesidad de la transferencia para la formulación, el ejercicio o la defensa de reclamaciones.
5. La necesidad de la transferencia para la protección de los intereses vitales del interesado o de otras personas por las que pueda dar su consentimiento.
6. La transferencia se realiza desde un registro público que tenga como finalidad facilitar información al público y esté abierto a cualquier persona, en general o con interés particular, en las formas establecidas por el Derecho de la UE o de los Estados miembros.

Fuera de estos casos, y de los arts. 45 y 46 RGPD, la transferencia solo podrá realizarse si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses, derechos o libertades del interesado y el interesado evaluó todas las circunstancias concurrentes y ofreció las garantías suficientes. Asimismo, se requiere que el responsable informe a la autoridad de control cuando se produzca esta transferencia. De esta forma, el último párrafo del art. 49.1 RGPD prevé lo que Castellanos Rodríguez[22] ha calificado como "cajón de sastre" al contradecir el objetivo principal de maximizar las garantías de protección de la norma europea

[22] Castellanos Rodríguez, A. (2017). *El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield*. Institut de Ciències Polítiques Socials *(UAB),* WP 350, p. 12.

permitiendo que las transferencias de datos personales se produzcan en aras de "intereses legítimos imperiosos" de una determinada empresa.

Como ha indicado Ruiz Tarrías[23], "la falta de concreción de la expresión "intereses imperiosos" genera dudas acerca de las transferencias internacionales a las que ofrecería cobertura legal, a pesar de que el Considerando 113 RGPD hace referencia al hecho de que deben ser tomadas en consideración "las legítimas expectativas" de la sociedad en un aumento del conocimiento para "fines de investigación científica o histórica o fines estadísticos". En todo caso, el Considerando subraya que únicamente puede utilizarse en "casos aislados".

De esta forma, de acuerdo con el CEPD[24], las excepciones deben interpretarse restrictivamente para su uso en situaciones específicas sin que se conviertan en la regla general y considerando que se debe poder demostrar por parte del responsable y el encargado de tratamiento que no era posible exportar los datos con garantías adecuadas ni dentro de las excepciones del art. 49.1 RGPD.

Por último, el art. 49.5 RGPD establece que en ausencia de decisión de adecuación, tanto la UE como los Estados miembros estarán habilitados para limitar la transferencia de categorías especiales de datos por razones de interés público.

2.6. El caso de Estados Unidos

Por otro lado, tenemos la situación concreta de Estados Unidos. En este caso, la Comisión Europea adoptó una Decisión de Adecuación para habilitar las trasferencias de datos internacionales para empresas que autocertificasen su protección de los datos personales y en cumplimiento de lo que se denominó "principios de puerto seguro".

No obstante, en la Sentencia Schrems[25] I, el TJUE dictaminó que la decisión de adecuación del marco del puerto seguro era inválida. En cuanto a las razones, el Tribunal consideró la falta de normas que limiten las injerencias en la vida privada, así como la

---

[24] Directrices 2/2018 sobre las excepciones contempladas en el artículo 49 del Reglamento 2016/679 Adoptadas el 25 de mayo de 2018. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_es.pdf (Consultado a 5 de junio de 2022).

[25] Schrems I op. cit. Véase: Uría Gavilán, E. (2016) Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems, *Revista de Derecho Comunitario Europeo*, Año nº 20, Nº 53, 2016, 261-282.

inexistencia de mecanismos de resolución de conflictos frente al Estado, junto con la conservación y tratamiento de datos transferidos de forma ilimitada.

Por otro lado, también se declaró la nulidad del art. 3 de la Decisión. La Directiva establecía que la autoridad de control sería competente para resolver sobre la compatibilidad de una Decisión de Adecuación y la propia Directiva. Al mismo tiempo, se limitaban en la Decisión las competencias de estas autoridades, contraviniendo lo estipulado en el art. 28 de la Directiva 95/46/CE.

Por todo ello, el TJUE declaró la nulidad de la Decisión y la falta de un nivel adecuado de protección, al contradecir los arts. 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea. Pues en realidad, en la Decisión, la Comisión solamente analizó el régimen de puerto seguro y no la existencia de un nivel de protección equivalente al de la UE en materia de protección de datos personales.

Como consecuencia de la decisión del TJUE, las compañías de EE.UU. adheridas al sistema de Puerto Seguro perdieron su condición de entidades adecuadas para ser destinatarias de transferencias de datos provenientes del EEE y tuvieron que buscar medios alternativos para realizar este tipo de transferencias. De tal modo, que se recurrió a las Cláusulas Contractuales Tipo (SCCs) y a las Normas Corporativas Vinculantes o *Binding Corporate Rules*. No obstante, ninguno de estos instrumentos es una alternativa real a la aplicación de un criterio de adecuación uniforme a todas las transferencias de datos desde la UE hacia los EE.UU.

En este marco, y en una situación difícil para las compañías, la UE y EE.UU. acordaron el Escudo de Privacidad UE-EE.UU. y, con fecha de 12 de julio de 2016[26], la Comisión declaró que los EE.UU. garantizaban un nivel adecuado de protección para los datos personales transferidos desde el EEE con destino a entidades estadounidenses.

A través de este acuerdo, se permitía que las empresas estadounidenses autocertificaran su adhesión vinculada al compromiso de cumplir las normas de protección de datos establecidas en el acuerdo. De esta forma, las autoridades de EE.UU. supervisaban y verificaban el cumplimiento de los compromisos acordados. Así, el nuevo instrumento de

[26] Decisión de ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 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., C(2016) 4176.

adecuación para las transferencias de datos personales hacia EE.UU. se denominó Escudo de Privacidad o *Privacy Shield.*

A pesar del ímpetu por retomar un marco legal que permitiese de forma general las transferencias de datos internacionales con EE.UU., el Escudo de Privacidad no incorporó grandes cambios en relación con el régimen de garantías del anterior puerto seguro. En esta línea, Gonzalo Domenech[27] lo ha llegado a calificar de "suave actualización", sobre todo en los pocos avances en la mejora de los principios de notificación y elección que ni siquiera alcanzan a operaciones típicas de procesamiento de datos como son la recopilación, el almacenamiento o la creación de perfiles.

Respecto a las diferencias principales con el sistema anterior, Brill[28] indica la creación de una figura dentro del Departamento de Estado estadounidense al que las autoridades de protección de datos presentarán peticiones en nombre de ciudadanos europeos. Asimismo, se planteó un sistema de revisión de la violación o falsificación de documentos y declaraciones en relación con el cumplimiento del *Privacy Shield* y se estableció un sistema de recursos y reclamaciones para los ciudadanos europeos. Por otro lado, se establecía la obligación de garantizar que las entidades vinculadas que reciben los datos de carácter personal de europeos también actuaban de conformidad con los principios del *Privacy Shield.*

El nuevo régimen, además de no aportar grandes cambios, no se vio exento de críticas, el Grupo de Trabajo del Art. 29, a través de los Documentos de Trabajo WP 237[29] y WP 238[30], criticó que la normativa estadounidense de protección de datos no resultaba de aplicación a los datos personales transferidos entre entidades privadas a través del Escudo de Privacidad a los que pueden tener acceso las autoridades estadounidenses. Esta situación se debía a que la Executive Order on Public Safety excluye la aplicación de la ley de protección de datos a personas extranjeras en EE.UU. Asimismo, en relación con

[27] Gonzalo Domenech, J. op. cit. p. 366.
[28] Brill, J. (2016). Strengthening international ties can support increased convergence of privacy regimes. *European Data Protection Law Review nº 2*, 155-156.
[29] Working Document (WP 237) 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) Adopted on 13 April 2016 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf (Consultado a 5 de junio de 2022).
[30] Working Document (WP 238) Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision Adopted on 13 April 2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (Consultado a 5 de junio de 2022).

las autoridades de control, la Oficina del Director de Inteligencia Nacional (ODNI) no excluía la recogida masiva e indiscriminada de datos personales de la UE.

Finalmente, la Decisión de Ejecución fue aprobada por la Comisión incluyendo entre sus considerandos valoraciones relacionadas con las insuficiencias del régimen anterior, así como la realización de un análisis sobre las prácticas vigentes en los EE.UU. y que llevó a la conclusión de que se garantizaba un nivel adecuado de protección.

A pesar de ello, no tardaron en surgir informes y resoluciones[31] desde las diferentes instituciones que planteaban una serie de recomendaciones que materializar como la designación de un Defensor del Pueblo Independiente.

Tras esta situación, el Sr. Schrems modificó su reclamación al considerar que el Derecho estadounidense imponía a Facebook el deber de poner a disposición de autoridades estadounidenses datos de carácter personal, vulnerando los arts. 7, 8 y 47 CDFUE. Consecuentemente, no se estaría cumpliendo con los requisitos necesarios para la realización de la transferencia internacional.

En la práctica, el demandante ponía en cuestión la validez de las cláusulas tipo que fueron adoptadas por la Comisión por medio de la Decisión 2010/87/UE al considerar que infringían la CDFUE.

En la Sentencia Schrems II, el TJUE puso de relieve que la existencia del Defensor del pueblo creado en el ámbito del Escudo de Privacidad no subsanaba las lagunas existentes por la imposibilidad de recurrir frente a injerencias de las autoridades estadounidenses. Por lo tanto, el TJUE consideró que la Comisión no pudo concluir de forma válida la existencia de un nivel de protección sustancialmente equivalente en EE.UU.

Asimismo, el alto Tribunal de Justicia diferencia claramente dos aspectos entre las garantías otorgadas con las decisiones de adecuación de las establecidas en virtud de cláusulas tipo.

En primer lugar, mientras las decisiones de adecuación no hayan sido declaradas inválidas por el TJUE, los Estados miembros y sus órganos no pueden adoptar medidas contrarias a las mismas. Por lo tanto, en principio, las autoridades nacionales de control no pueden

[31] Veáse el Informe de la Comisión sobre la primera revisión anual del funcionamiento del Escudo de la privacidad UE–EE.UU (COM(2017) 611 final); El Documento de Trabajo (WP 255) del Grupo de Trabajo del Art. 29 adoptado en el primer año de vigencia del escudo o la Resolución del Parlamento Europeo de 5 de julio de 2018u (PE, 2018a).

adoptar medidas que las cuestionen, si bien, no se puede impedir que un interesado presente una reclamación ante la autoridad de control correspondiente.

Sin embargo, cuando la transferencia de datos se base en otro tipo de legitimación como es el caso de las cláusulas tipo, de acuerdo con el art. 4 de la Decisión de Ejecución 2010/87/UE, las autoridades de control tienen la facultad de prohibir o suspender una transferencia de datos personales cuando verifiquen que suponga una infracción del Derecho de la Unión o de la normativa estatal en la materia.

En segundo lugar, en cuanto al nivel de protección de las transferencias internacionales fundadas en cláusulas tipo, el TJUE considera que las garantías adecuadas a efectos del art. 45 RGPD —lo que incluye las realizadas en virtud de una decisión de adecuación y las acogidas a una cláusula tipo— gozan de un nivel sustancialmente equivalente al garantizado en la UE. Por lo tanto, resulta exigible constatar la existencia de garantías adecuadas en ambos tipos de mecanismos.. No obstante, el TJUE introduce una diferencia sustantiva, y es que, en el caso de las cláusulas tipo, hay que valorar exclusivamente las estipulaciones contractuales entre el encargado/responsable y el destinatario de la transferencia a la hora de determinar la existencia de un nivel adecuado de protección. Si bien, no hay que olvidar que este tipo de cláusulas pueden ser suspendidas o prohibidas si no respetan las garantías exigidas o resultan de imposible cumplimiento por las autoridades de control competentes.

Por otro lado, en relación con la primacía que otorga el Escudo de Privacidad a las cuestiones de seguridad nacional, interés público y cumplimiento de la ley, el TJUE considera que el art. 1.1 de la Decisión de adecuación 2016/1250 no tuvo en consideración los elementos del art. 45.1 RGPD interpretados conforme a la CDFUE. Asimismo, esta invalidez se extiende al conjunto de la Decisión de Ejecución 2016/1250 debido a la conexión del precepto con los arts. 2 a 6 y Anexos.

De esta forma, a través de la Sentencia Schrems II[32], el TJUE considera que la Decisión Escudo de Privacidad es inválida de acuerdo con las exigencias que derivan del marco normativo en materia de protección de datos en la UE y su interpretación de conformidad con la Carta de los Derechos Fundamentales de la UE, y principalmente, de acuerdo con el respeto a la vida privada y familiar, la protección de los datos de carácter personal y el derecho a la tutela judicial efectiva. Por lo tanto, al reconocer la citada Decisión la

[32] Schrems II op. cit.

primacía de las exigencias relativas a seguridad nacional, interés público y cumplimiento de la ley de EE.UU., se posibilitan injerencias en los Derechos Fundamentales de las personas cuyos datos se están transfiriendo. Asimismo, añade que el mecanismo del Defensor del Pueblo de la Decisión no ofrece garantías sustancialmente equivalentes a las garantizadas por el Derecho de la Unión.

Como indica Monika Zalnieriute[33], la Sentencia Schrems II pone de manifiesto la necesidad de un replanteamiento de la vigilancia y la protección de datos en Estados Unidos sin la cual la UE se arriesga a permitir violaciones de los derechos reconocidos en la CDFUE. No obstante, a pesar de que Schrems II reafirma la necesidad de proteger los derechos de los ciudadanos, su impacto político podría ser muy similar al de Schrems I. No hay que olvidar la interdependencia económica entre los Estados Unidos y la UE que impide la suspensión a nivel global de las transferencias de datos entre ambos países.

La Sentencia tiene consecuencias de gran alcance en todos los instrumentos jurídicos utilizados para transferir datos personales desde el EEE a cualquier tercer país. En este contexto, el Supervisor Europeo de Protección de Datos[34] (SEPD) pretende que todas las transferencias se ajusten a la sentencia a medio plazo. Si bien, ha determinado dos prioridades que deben abordarse a corto plazo: los contratos en curso entre el responsable y el encargado del tratamiento y/o los contratos entre el encargado y el subencargado del tratamiento que implican transferencias de datos a terceros países, con especial énfasis en las realizadas a los Estados Unidos.

En este contexto, el SEPD ha elaborado un plan de acción para racionalizar las medidas de cumplimiento y ejecución, distinguiendo entre las acciones de cumplimiento a corto y a medio plazo.

Mientras se sigue aplicando la Estrategia, el Supervisor ha realizado un llamamiento a las instituciones de la UE para que eviten las transferencias de datos personales hacia los Estados Unidos para nuevas operaciones de tratamiento o nuevos contratos con proveedores de servicios.

---

[33] Zalnieriute, M. (2022). Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security (April 14, 2021*). Vanderbilt Journal of Transnational Law, (2022) 55(1), p. 45-48.* https://ssrn.com/abstract=3826878 (Consultado a 5 de junio de 2022).

[34] Supervisor Europeo de Protección de datos: Strategy for EU institutions to comply with "Schrems II" Ruling. https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en (Consultado a 5 de junio de 2022).

Por su parte, el CEPD[35] ante la situación provocada por el fallo del TJUE considera aceptable la utilización de las excepciones previstas en el art. 49 RGPD para permitir las transferencias de datos siempre y cuando se garantice el cumplimiento de los términos dictados en las Directrices 2/2018, resaltando su carácter ocasional y no repetitivo. Al mismo tiempo, se admite la utilización de cláusulas contractuales tipo de protección de datos siempre y cuando se evalúen caso por caso y atendiendo a las circunstancias de las transferencias.

En esta línea y dada la gran transcendencia del tráfico de datos en la UE y EE.UU., la Comisión y las instituciones americanas se han puesto a negociar un nuevo marco que facilite las transferencias internacionales de datos personales. De esta forma, recientemente anunciaron un principio de acuerdo para un Marco Transatlántico de Privacidad de Datos[36] y que como novedad incluye el compromiso de EE.UU. para implementar reformar en materia de protección de datos.

IV. LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES: REGLAMENTO 2018/1807, RELATIVO A UN MARCO PARA LA LIBRE CIRCULACIÓN DE DATOS NO PERSONALES EN LA UNIÓN EUROPEA

La materia se ha regulado por medio del Reglamento (UE) 2018/1807[37] relativo a un marco para la libre circulación de datos no personales en la Unión Europea[38]. Así, de acuerdo con los considerandos del Reglamento, éste toma como base el papel que juega la digitalización y las tecnologías de la información y la comunicación en todos los sistemas económicos e innovadores modernos y la consecuente necesidad de dar solución a los nuevos problemas jurídicos en torno a las cuestión del acceso a los datos y su

[35] Comité Europeo de Protección de Datos. Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf (Consultado a 5 de junio de 2022).

[36] Así se ha comunicado por ambas instituciones en sus respectivos comunicados de prensa. Veáse: The White House: FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework. Accesible en: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ (mayo de 2022) (Consultado a 5 de junio de 2022). y Comisión Europea: European Commsion and United States Joint Statement on Trans-Atlantic Data Privacy Framework. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (Consultado a 5 de junio de 2022).

[37] Reglamento (UE) 2018/1907 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018 relativo a un marco para la libre circulación de datos no personales en la Unión Europea DOUE L 303/59 de 28 de noviembre de 2018.

[38] Jarne Muñoz, P. (2019). Algunas reflexiones acerca de la propuesta de reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. *¿Cómo poner en práctica el gobierno abierto?*, Editorial Reus, pp. 51-64.

reutilización, la responsabilidad, la ética y la solidaridad. De esta forma, la libre circulación de datos es fundamental para alcanzar un crecimiento e innovación y es por ello por lo que uno de los fines del Reglamento es crear un marco para la libre circulación de estos datos en el ámbito de la Unión Europea que permita el desarrollo de la economía de los datos y la mejora de la competitividad. En este sentido, los datos juegan un papel fundamental para avanzar en la consecución de un Mercado Único Digital.

Ha sido profundamente analizada la protección de los datos de carácter personal. No obstante, en el caso de aquellos datos que no son personales, la privacidad deja de llevar el peso central en la materia virando hacia aspectos económicos, empresariales o estadísticos.

En lo que respecta al propio Reglamento, el art. 1 indica que tiene por objeto garantizar la libre circulación de datos no personales a través de un conjunto de normas para los usuarios profesionales.

En lo que respecta al ámbito de aplicación de la norma, se aplica al tratamiento de datos no personales prestado como un servicio a usuarios que residan o tengan un establecimiento en la Unión con independencia de que el proveedor de servicios este establecido en la Unión y al tratamiento de datos no personales efectuado por personas físicas o jurídicas que residan o tengan un establecimiento en la Unión (art. 2.1 Reglamento).

En cuanto a la libre circulación de datos en la Unión, en el art. 4 se prohíbe la existencia de requisitos para la localización de datos, entendiendo como tal conforme a la definición dada por el Reglamento: “cualquier obligación, prohibición, condición, restricción u otro requisito previsto en cualquier disposición normativa o administrativa de los Estados miembros que imponga el tratamiento de datos en el territorio de un determinado Estado miembro o dificulte el tratamiento de datos en cualquier otro Estado miembro”.

De tal forma que se establece la obligación de los Estados miembros de comunicar a la Comisión cualquier proyecto de acto que plantee un nuevo requisito de localización de datos o modifique uno existente. Asimismo, se estableció como fecha límite el 30 de mayo de 2021 para derogar cualquier tipo de requisito existente de localización por parte de los Estados miembros o respecto de aquellos conferidos sobre la base del Derecho vigente de la Unión para aportar la oportuna justificación para mantenerla vigente.

Por otro lado, de conformidad con el art. 5 del Reglamento, no quedan afectadas las competencias de las autoridades de solicitar u obtener acceso a datos en el desempeño de sus funciones y se prevé la posibilidad de solicitar asistencia entre autoridades de diferentes Estados miembros.

En cuanto a la portabilidad de datos, desde la Comisión se fomentará y facilitará la elaboración de códigos de conducta autorreguladores que tengan por objeto el desarrollo de una economía de datos competitiva y basada en los principios de interoperabilidad y transparencia.

También se incluye un artículo dedicado a la cooperación entre autoridades a través de puntos de contacto únicos y se establece que con fecha límite el 29 de noviembre de 2022 la Comisión deberá presentar un informe al Parlamento Europeo y al Consejo donde evalúe la aplicación del presente reglamento, y más concretamente, la aplicación del art. 4.1 sobre la prohibición de requisitos de localización y la elaboración y aplicación efectiva de Códigos de Conducta y suministro de información al amparo del art. 6.

De esta forma, se ha establecido el marco legal para el desarrollo de transferencias internacionales de datos, si bien, futuros desarrollos son necesarios en lo que respecta a la protección de este tipo de transferencias. Asimismo, la materia hay que encuadrarla dentro de la Estrategia Europea de Datos que se va a analizar en el próximo apartado y que plantea las actuaciones a llevar a cabo por las instituciones europeas en el ámbito de los datos durante los próximos años.

V. UNA ESTRATEGIA EUROPEA DE DATOS. ESPECIAL MENCIÓN A LA PROPUESTA DE REGLAMENTO RELATIVO A LA GOBERNANZA EUROPEA DE DATOS

Con el aumento de las tecnologías de la información y la comunicación se ha producido una gran transformación en la economía y sociedad a nivel global y en el día a día de todos los ciudadanos europeos. En esta transformación cobran un papel fundamental los datos, su tratamiento y sus innumerables beneficios para los ciudadanos que van desde una medicina más personalizada o la mejora del bienestar hasta incremento de la productividad y el aumento de la competitividad de los mercados europeos.

Por medio de la Comunicación de la Comisión relativa a Una Estrategia Europea de Datos[39], se plantea el plan de acción sobre medidas políticas e inversiones que hagan posible la economía de los datos de los cinco años siguientes a su publicación, es decir, hasta 2025.

Asimismo, sobre la base de esta Estrategia, se pone en marcha una consulta sobre las medidas específicas necesarias para mantener a Europa como uno de los motores en el uso y tratamiento de datos junto con el respeto y defensa de los valores y principios fundamentales de la Unión.

En el contexto actual, el volumen de datos está creciendo año tras año y los beneficios e importancia de los datos son notables para la economía y sociedad. Asimismo, las fuentes de competitividad para las próximas décadas se deciden en el momento actual. Y es la UE quien tiene el potencial para tener éxito en una economía ágil en el manejo de datos. No obstante cuenta con importantes rivales como son China y EE.UU.

Para hacer frente a esta situación, hay que encontrar un modo propio de equilibrar el flujo y el uso de datos junto con el respeto de la privacidad, la protección, la seguridad y la ética. Esta visión de la Comisión se encuadra con los valores y derechos fundamentales europeos.

En este contexto, la UE debe crear un entorno político con el objeto de que su cuota en la economía de datos represente al menos su peso económico, y además, que se trate de elecciones libres, y no por imposición a las empresas. Para ello, la estrategia pasa por la creación de un espacio único europeo de datos, de tal forma que se cree un mercado único abierto a datos de cualquier parte del mundo y donde se garantice la seguridad y su acceso, impulsando el crecimiento y la creación de valor, junto con la minimización del impacto medioambiental y de carbono.

En lo que respecta al marco legal, se requiere una normativa que pueda aplicarse de forma eficaz y se garantice la conformidad con las nomas del mercado único de la UE. Todo pasa por la combinación y adaptación de la legislación y gobernanza para la garantía de la disponibilidad de datos y la existencia de normas, herramientas e infraestructuras que permitan el manejo de los datos.

[39] Comunicación (COM(2020) 66 final) de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una Estrategia Europea de Datos.

De esta forma, se persigue que las normas europeas y sus mecanismos de aplicación garanticen que los datos puedan fluir en la UE, independientemente del sector, con pleno respeto a las normas y valores europeos y en especial a la legislación de protección de datos personales, de protección del consumidor y de defensa de la competencia. Asimismo, que las normas sean justas, prácticas y claras, con un enfoque abierto y con mecanismos claros y fiables de gobernanza de datos.

Para lograr los objetivos planteados, se requiere de la suficiente capacidad de inversión en tecnologías e infraestructuras, competencias digitales y alfabetización en materia de datos.

No obstante, en la actualidad nos encontramos con una serie de problemas como es el caso de la disponibilidad de los datos y su calidad, los desequilibrios en el poder de mercado, la gobernanza de datos o las infraestructuras y tecnologías de datos necesarias, así como la falta de cualificación e la materia, entre otros.

1. LA ESTRATEGIA

Tiene como objeto sentar las bases y el camino para la creación y materialización de un mercado único de datos, a través de las medidas legislativas y financiación requerida.

Por un lado, nos encontramos con medidas transversales que tienen por objeto el acceso a los datos y su utilización en el contexto de un mercado global que facilite el ágil manejo de los datos. Para ello, se pretende poner en marcha un marco legislativo propicio para la gobernanza de los espacios comunes europeos. Por medio de este marco, se busca reforzar las estructuras necesarias, tanto para los Estados miembros como a nivel de la Unión lo que permitirá facilitar el uso de datos por parte de las empresas con fines innovadores y con el objeto de reforzar los mecanismos de gobernanza a nivel europeo y de los Estados miembros y facilitar el uso de los datos.

Por otro lado, la Comisión busca facilitar un mayor volumen de datos de calidad del sector público para su reutilización. Para ello, se iniciará el procedimiento para la adopción de un acto de ejecución sobre conjuntos de datos de gran valor en el marco de la Directiva sobre datos abiertos, permitiendo la disponibilidad de los mismos de forma gratuita y facilitando su acceso.

Asimismo, se ha estudiado la necesidad de adoptar medidas legislativas sobre las cuestiones que afectan a las relaciones entre los actores de una economía ágil en el manejo

de datos con el objetivo de incentivar las relaciones e intercambios de datos entre diferentes sectores.

Para la materialización de la Estrategia, la Comisión invertirá para el periodo (2021-2027) en un proyecto de gran impacto sobre los espacios de datos europeos y las infraestructuras de computación en la nube. De esta forma, se apoyará la creación de infraestructuras, herramientas y mecanismos de gobernanza con vistas a unos ecosistemas florecientes para la puesta en común de datos y la inteligencia artificial. Respecto al proyecto, este se basará en la federación europea, es decir, interconexiones de infraestructuras en la nube y en el borde eficientes.

Según las estimaciones que plantea la Comisión en la citada Comunicación, se estima una inversión de entre 4.000 y 6.000 millones entre Estados miembros, Comisión y la industria. Este modelo busca reunir a agentes públicos y privados para el desarrollo de plataformas comunes que ofrezcan acceso a los servicios en la nube que permitirán el almacenamiento e intercambio de datos, así como el desarrollo de nuevos recursos digitales.

Asimismo, se pretenden aprovechar las sinergias que se generen entre el trabajo sobre la federación en la nube europea y las iniciativas de los Estados miembros, buscando evitar la fragmentación y fomentando el entendimiento entre los países.

En definitiva, se pretende convertir a la UE en una economía ágil en el manejo de datos y que garantice un alto grado de seguridad y facilidad en el acceso de datos. Asimismo, la Estrategia también plantea la creación de espacios europeos de datos en sectores estratégicos y en ámbitos de interés público. Este es el caso, de los siguientes espacios:

1. Espacio común europeo de datos relativos a la industria.
2. Espacio común europeo de datos relativos al Pacto Verde.
3. Espacio común europeo de datos relativos a la movilidad.
4. Espacio común europeo de datos relativos a la salud.
5. Espacio común europeo de datos en materia financiera.
6. Espacio común europeo de datos relativos a la energía.
7. Espacio común europeo de datos relativos al sector agrario.
8. Espacio común europeo de datos relativos a las administraciones públicas.

9. Espacio común europeo de datos en materia de cualificaciones.

Al mismo tiempo, la Nube europea de la Ciencia Abierta ofrecerá un acceso fluido a los datos de investigación gracias a un entorno de datos abierto y de confianza y los servicios conexos.

En lo que respecta a la gobernanza de datos, el 25 de noviembre de 2020, la Comisión Europea presentó la Propuesta de Reglamento relativo a la gobernanza europea de datos (LGD)[40]. De esa forma, se presenta la primera de las medidas anunciadas en la Estrategia Europea de Datos de 2020 y que tiene por objetivo ampliar la disponibilidad y la utilización de datos, poniendo especial hincapié en la confianza en los intermediarios de datos y el refuerzo de los mecanismos para el intercambio de datos en el conjunto de la UE.

De esta forma, el instrumento aborda:

- La cesión de datos del sector público para su reutilización, en los casos en que esos datos estén sujetos a derechos de terceros.
- El intercambio de datos entre empresas a cambio de algún tipo de remuneración.
- La cesión de datos personales con ayuda de un intermediario de datos personales.
- La cesión de datos con fines altruistas.

Asimismo, esta iniciativa se encuadra dentro del marco regulatorio que ya se ha descrito con anterioridad, en especial el RGPD, la Directiva sobre privacidad y las comunicaciones electrónicas y viene a completar la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertas y la reutilización de la información del sector público (Directiva sobre datos abiertos).

Además, se continúa el proceso de adopción y preparación de legislación sectorial relativa al acceso a los datos de determinados ámbitos, como pueden ser el de proveedores de pago, la red eléctrica o la información medioambiental.

La Propuesta se plasma en 8 Capítulos. En el Capítulo I, bajo la rúbrica de Disposiciones Generales se define el objeto y el ámbito de aplicación del Reglamento. Así, se establecen las condiciones para la reutilización en el ámbito de la UE de determinadas categorías de

[40] Comunicación (COM(2020) 767 final 2020/0340 (COD)) de la Comisión Europea: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), de 25 de noviembre de 2020.

datos conservados por el sector público, junto con un marco de notificación y supervisión de los servicios de intercambio de datos y un registro de las entidades que con fines altruistas recojan y traten datos. Por otro lado, el art. 2 presenta las definiciones que serán empleadas a lo largo de la Propuesta.

A continuación, el Capítulo II se dedica a la reutilización de determinadas categorías de datos protegidos debido a su confidencialidad —comercial o estadística—, o por tratarse de datos personales o protegidos por los derechos de propiedad intelectual de terceros y que se encuentren conservados por organismos del sector públicos.

De esta forma, se plantean una serie de condiciones en las que se permite su reutilización, y, por regla general, se prohíben los acuerdos de exclusividad. Mientras que en el artículo quinto se establece que los organismos del sector público que, en virtud del Derecho nacional, sean competentes para conceder o denegar el acceso a efectos de reutilización, publicarán las condiciones en las que se permite la reutilización. No obstante, estas condiciones no podrán establecer ningún tipo de discriminación, serán proporcionadas y estarán justificadas objetivamente, sin que ninguna de las condiciones pueda restringir la competencia.

También se dedica un artículo a la designación por parte de los Estados miembros de organismos competentes para asistir a los organismos del sector público a través del apoyo técnico. Además, se establecerá por parte de cada Estado miembro un punto de contacto único de apoyo a investigadores y empresas innovadoras en la identificación de datos adecuados y en la implantación de estructuras de apoyo a los organismos del sector público con medios técnicos y asistencia jurídica.

El Capítulo III regula los requisitos aplicables a los servicios de intercambio de datos. En primer lugar, se sujeta la prestación de los servicios de intercambio de datos a un procedimiento de notificación ante la autoridad competente. En segundo lugar, el art. 11 establece las condiciones para la prestación de servicios de intercambio de datos y que son las siguientes:

1. Los proveedores no podrán hacer uso de los datos más allá de su puesta a disposición para los usuarios de datos.
2. Los metadatos recogidos solo podrán utilizarse para la prestación del servicio de intercambio de datos.

3. Los proveedores velarán porque su servicio y acceso sea equitativo, transparente y sin discriminación.
4. El intercambio de datos entre proveedores será en el mismo formato y únicamente se convertirán los datos en formatos específicos con el objeto de mejorar la interoperabilidad o a solicitud del usuario, por exigencia de la Unión o a efectos de armonización de normas internacionales.
5. Los proveedores tendrán procedimientos para impedir prácticas abusivas o fraudulentas.
6. Los proveedores velarán por la continuidad del servicio y establecerán los mecanismos necesarios a tal fin.
7. Los proveedores aplicarán las medidas necesarias con el fin de evitar el acceso o transferencia de datos contrario al Derecho de la Unión.
8. Los proveedores garantizarán un elevado nivel de seguridad en el almacenamiento y transmisión de datos no personales.
9. Los proveedores aplicarán procedimientos para garantizar el cumplimiento del Derecho de competencia nacional y europeo.
10. Los proveedores actuarán en el mejor interés de los usuarios y facilitarles el ejercicio de sus derechos.
11. Los proveedores proporcionarán herramientas para obtener el consentimiento o el permiso para tratar los datos facilitados por personas jurídicas.

De esta forma, se busca asegurar un funcionamiento de los servicios de datos abierto y colaborativo que permita el empoderamiento de las personas, tanto físicas como jurídicas, garantizándoles una visión general y un mejor control sobre sus datos.

En el Capítulo IV, se presenta la cesión de datos con fines altruistas por medio de un registro de organizaciones reconocidas de gestión de datos con estos fines. Para ello, la puesta a disposición de datos para el bien común deberá hacerse de forma voluntaria, tanto por particulares como por empresas, y a través de organizaciones registradas. Asimismo, se elaborará un formulario de consentimiento para la cesión altruista de datos que permita reducir los costes que requiere recabar el consentimiento.

Por otro lado, el Capítulo V se encarga del funcionamiento de las autoridades competentes dedicadas al seguimiento y aplicación del procedimiento de notificación que resulta de aplicación a las entidades prestatarias del servicio de intercambio de datos y a aquellas que desempeñen las actividades de cesión altruista de datos. Asimismo, se reconocen los derechos de reclamación ante la autoridad nacional competente y a la tutela judicial efectiva en el marco de la presente propuesta.

A continuación, por medio del Capítulo VI se crea el Comité Europeo de Innovación en los Datos como un grupo de expertos que tiene por objeto el asesoramiento y asistencia a la Comisión en el desarrollo de actuaciones coherentes con la normativa en la materia y en especial la recogida en los Capítulos ya mencionados del Reglamento.

Por último, el Capítulo VII permite a la Comisión la adopción de actos de ejecución en relación con el formulario europeo de consentimiento para la cesión altruista de datos y el Capítulo VIII establece un régimen transitorio para la autorización de los proveedores de servicios de intercambio de datos y una serie de disposiciones finales.

Para finalizar, en relación con las transferencias de datos, en el ámbito de los datos no personales también resulta importante su protección. No hay que olvidar que entre ellos se encuentran los datos comerciales, datos protegidos por derechos de propiedad intelectual, entre otros. De esta forma, cobran especial relevancia otro tipo de derechos fundamentales como es el caso del derecho de propiedad.

Para asegurar su protección, es necesario que los datos no personales que obren en poder de organismos del sector público solamente puedan transferirse a terceros países que ofrezcan garantías adecuadas para su utilización. Con este objetivo, la Comisión puede adoptar actos de ejecución que declaren que el tercer país ofrece un nivel de protección equivalente al garantizado en la Unión. Este régimen se asemeja al de las decisiones de adecuación para transferencias de datos de carácter personal.

Cuando no exista el acto de ejecución de la Comisión que ofrezca este tipo de garantías de protección equivalentes, el organismo del sector público únicamente debe transmitir los datos protegidos a un reutilizador cuando este contraiga obligaciones en interés de la protección de los datos. Para la transferencia de datos por parte del reutilizador se requerirá del compromiso de cumplimiento de las obligaciones establecidas en el reglamento y se deberá aceptar por lo que respecta a la resolución judicial de litigios, las competencias del Estado miembro al que pertenezca el organismo del sector público que haya permitido la reutilización.

Por lo tanto, el régimen de transferencias previsto en la Ley de Gobernanza de Datos es, en cierta medida, limitado. Faculta a la Comisión para determinar si las leyes de propiedad intelectual y de secretos comerciales de los distintos terceros países son equivalentes a las de la UE. En ausencia de estas decisiones, las transferencias a un tercer país solamente podrán realizarse si el reutilizador asume contractualmente responsabilidad para salvaguardar la propiedad intelectual y los secretos comerciales. Mientras que las transferencias internacionales de datos sensibles, como podrían ser los relacionados con la salud, podrían ser prohibidos de forma rotunda. Asimismo, el CEPD[41] plantea una serie de deficiencias —e insta a los colegisladores a tenerlas en cuenta— que se indican a continuación:

La interacción entre la LGD y el RGPD. Así, las definiciones y la terminología que ha sido utilizada en la LGD precisan de su armonización en consonancia con las estipulaciones del RGPD. En especial, las definiciones introducidas por la LGD, en la medida en que resultan de aplicación al tratamiento de datos personales, no deben resultar incompatibles con el RGPD. De tal forma que resulta necesario que en la definición de los conceptos "datos personales", "interesado", "consentimiento" y "tratamiento" se establezca una remisión al RGPD, mientras que en el caso de "metadatos", "titular de los datos", "usuario de datos", "intercambio de datos" y "altruismo de datos" se deben modificar de forma que resulten coherentes con el marco legal establecido.

Por otro lado, la LGD debe aclarar que el tratamiento de datos personales debe basarse en un fundamento jurídico adecuado (art. 6 RGPD) o en una excepción de las previstas en el art. 9 RGPD. Asimismo, es necesario especificar si las disposiciones de la LGD se refieren a datos personales, no personales o a ambos. En este sentido, en el caso de tratarse de conjuntos de datos mixtos, la Comisión[42] ha considerado que se encuentran vinculadas a la aplicación del RGPD.

En lo que respecta a las autoridades para la protección de datos personales y para facilitar la libre circulación de datos personales, conforme al art. 16.2 TFUE, debe reflejarse en la LGD que son aquellas establecidas en el RGPD.

[41] Declaración 05/2021 sobre la Ley de gobernanza de datos a la luz de la evolución legislativa, adoptada el 19 de mayo de 2021.
[42] Comunicación de la Comisión al Parlamento Europeo y al Consejo Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. COM/2019/250 final.

Asimismo, se critican una serie de disposiciones del texto que sugieren la idea de legitimar el comercio de datos, lo que resulta incompatible con el carácter personal del derecho a la protección de datos personales y es que en ningún caso cabe considerar una "mercancía" a los datos personales.

Por otro lado, en relación con las organizaciones altruistas, se deben imponer los mismos requisitos que a las restantes organizaciones con el objeto de que se evite el aprovechamiento de esta denominación para obtener el consentimiento al tratamiento de datos personales.

El CEPD considera que el régimen previsto de notificación —o registro, en el caso de organizaciones altruistas— no prevé un procedimiento de investigación suficientemente riguroso. Por lo tanto, se recomienda contemplar la inclusión de procedimientos de rendición de cuentas y compromiso de cumplimiento en el tratamiento de datos personales conforme al RGPD, como la adhesión a un código de conducta o a un mecanismo de certificación.

Para finalizar, hay que añadir que la LGD no ha concretado que se entiende por "fines de interés general", por lo tanto, resulta un concepto que requiere de una definición más precisa.

En definitiva, se han valorado una serie de deficiencias que deben ser resueltas con objeto de evitar que la LGD establezca un marco normativo paralelo y sin coherencia con el RGPD y con el resto del Derecho de la Unión.

En el mismo sentido, en noviembre de 2021, el Comité Europeo de Protección de Datos[43] criticó las propuestas presentadas por la Comisión desde noviembre de 2020. Así, considera que las propuestas de Ley de Servicios Digitales (LSD)[44], la Ley de Mercados Digitales (LMD)[45], la Ley de Gobernanza de Datos (LGD)[46] y el Reglamento sobre un

[43] Declaración sobre el paquete de servicios digitales y la estrategia de datos, adoptada el 18 de noviembre de 2021.

[44] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de Servicios Digitales) y por el que se modifica la Directiva 2000/31/CE. COM/2020/825 final.

[45] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales). COM/2020/842 final.

[46] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos). COM(2020) 767 final.

enfoque europeo en materia de inteligencia artificial (RIA)[47] que tienen por objetivo fomentar un mayor y mejor uso y transmisión de datos entre agentes públicos y privados dentro de lo que se ha denominado como la economía de datos y que permitirá apoyar el uso y desarrollo de nuevas tecnologías como el Big Data y la Inteligencia Artificial, en su redacción actual, pueden no crear las condiciones para la innovación y el crecimiento económico que buscan.

El CEPD considera las propuestas faltas de protección de los derechos y libertades fundamentales de las personales. Asimismo, en relación con las autoridades de control independiente, las autoridades de control de la protección de datos no son designadas como las principales autoridades independientes. Más aún si cabe, cuando el art. 16.2 TFUE y el art. 8.3 de la CDFUE, requieren que la supervisión del tratamiento de datos personales recaiga sobre autoridades independientes de protección de datos. Tampoco se establece en las diferentes propuestas la cooperación entre los organismos de control y las autoridades de control de la protección de datos y no se aborda de forma adecuada las situaciones de posibles solapamientos de competencias. De tal forma que existe un importante riesgo de creación de estructuras de cooperación paralelas sin una coordinación y cooperación estructurada entre ellas.

Por lo tanto, se precisa que cada propuesta regule de forma clara y precisa a las autoridades de protección de datos competentes y se establezca una base jurídica suficiente para el intercambio de información necesaria con el fin de realizar una cooperación eficaz y determinar las circunstancias en que debe llevarse a cabo tal cooperación.

Para concluir, la parte dispositiva de las propuestas puede crear cierta ambigüedad en relación con la aplicación del marco de protección de datos en determinados casos. Es por ello, por lo que se requiere que se indique claramente que las nuevas propuestas no afectarán a la aplicación de las normas vigentes y garantizarán la prevalencia de las normas de protección de datos.

Finalmente, el 3 de junio de 2022 se publicaba en el DOUE el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de Mayo de 2022 relativo a la gobernanza europea

[47] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la unión. COM/2021/206 final.

de datos y por el que se modifica el Reglamento (UE) 2018/1724. El citado Reglamento mantiene la visión y estructura planteadas por la Propuesta de la Comisión, si bien incorpora algunas modificaciones. En este sentido, hay que mencionar que el texto pasa de 35 a 38 artículos, esto se debe a que aporta mayor claridad y descripción en los preceptos. De esta forma, en el artículo noveno del Reglamento se regula el procedimiento de solicitud de reutilización que si bien se contenía en el artículo octavo de la Propuesta, ahora dispone de un precepto propio dedicado a ello en exclusiva. Por otro lado, en el art. 16 del Reglamento se establece la posibilidad de que los Estados miembros establezcan disposiciones organizativas, técnicas o ambos tipos para facilitar la cesión altruista de datos.

Por último, en el art. 22 del Reglamento se habilita a la Comisión para adoptar un código normativo que instaure los requisitos de información, técnicos y de seguridad adecuados para recabar el consentimiento, así como garantizar un nivel de seguridad apropiado, junto con hojas de ruta sobre comunicación y recomendaciones que sean pertinentes. Asimismo, hay que hacer mención a que este Reglamento será de aplicación a partir del 24 de septiembre de 2023.

2. SITUACIÓN ACTUAL

A finales de noviembre del año 2021, el Consejo y el Parlamento Europeo publicaron que se había llegado a un acuerdo provisional para materializar la propuesta de Ley de Gobernanza de Datos que permitirá promover la disponibilidad de datos y crear un entorno fiable, facilitando su uso en investigación y la creación de nuevos productos y servicios innovadores.

Como indicó el Ministro de Administración Pública de Eslovenia y Presidente del Consejo[48]: "La Ley de Gobernanza de Datos es un hito importante que impulsará la economía de los datos en Europa en los próximos años. Al permitir el control y crear confianza, contribuirá a liberar el potencial de enormes cantidades de datos generados por las empresas y los particulares. Esto es indispensable para el desarrollo de aplicaciones de inteligencia artificial y vital para la competitividad de la UE a nivel mundial en este ámbito. Las innovaciones basadas en datos nos ayudarán a hacer frente a una serie de retos sociales y a impulsar el crecimiento económico, que es tan importante para la recuperación posterior a la COVID".

[48] Consilium (2021): Promoting data sharing: presidency reaches deal with Parliament on Data Governance Act.

Más recientemente, concretamente, el 23 de marzo de 2022, la Comisión Europea presentó una propuesta de Ley de Datos[49] que constituye la última de sus actuaciones en el ámbito de la Estrategia Europea de Datos y que viene a completar a las propuestas ya presentadas con anterioridad —LSD, LMD, LGD y RIA—.

Ante el creciente volumen de datos generado en los últimos años, la mayor parte de los mismos recaen de forma concentrada en unas pocas grandes compañías. Por el contrario, gran parte de todos los datos podría ser beneficioso y reutilizado entre los diferentes sectores. De esta forma, la Comisión plantea el objetivo de que los datos sean compartidos, almacenados y procesados en la Unión Europea y conforme a los principios y reglas propias de nuestro territorio común. Todo ello permitirá obtener la soberanía europea en materia de datos e innovación[50].

Los datos que se busca que sean objeto de tratamiento son los generados por máquinas y dispositivos, utilizados de forma no personal. Para ello, se requiere, en primer lugar, que se establezcan las reglas y propósitos sobre el control y uso de este tipo de datos.

No obstante, a pesar de centrarse en esta tipología de datos, el ámbito de la Ley de Datos alcanzará, tanto aquellos de carácter personal como no personal, sin que en ningún caso quede desplazado el RGPD. De esta forma, la nueva norma operará como un régimen paralelo y relativo a los derechos de tipo económico en lugar de los derechos fundamentales protegidos por el RGPD.

Asimismo, la nueva propuesta persigue que los servicios de almacenamiento de datos sean accesibles también para la pequeña y mediana empresa que había quedado desplazada debido a los altos precios de los grandes proveedores de este tipo de servicios.

En conclusión, tal y como opina Propp[51], la Ley de Datos puede tener un recorrido más lento y difícil que la Ley de Gobernanza de Datos, debido a su amplio alcance y a la mayor variedad de intereses corporativos y sociales afectados. La eficacia de algunos de sus elementos más innovadores, como el refuerzo del poder negociador de las empresas

[49] Comunicación de la Comisión: COM(2022) 68 final: Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (Ley de Datos).

[50] Sobre la soberanía digital de la UE véase Christakis, T. (2020) *European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy*. Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute. Disponible en: http://dx.doi.org/10.2139/ssrn.3748098 (Consultado a 5 de junio de 2022).

[51] Propp, K. (2022). Cultivating Euope's Data Garden. *Lawfare.* https://www.lawfareblog.com/cultivating-europes-data-garden. (4 de marzo de 2022). (Consultado a 5 de junio de 2022).

que pretenden reutilizar los datos no personales de otras empresas, está por ver. Sin embargo, lo que ya es seguro es que estas medidas de gobernanza de datos son mucho más sistemáticas que cualquier otra cosa que se haya intentado antes y que, por lo tanto, podrían estimular los esfuerzos legislativos en otros lugares[52].

Las respuestas extranjeras a estos esfuerzos para construir la gobernanza de los datos inevitablemente se verán influenciadas por sus capacidades restrictivas de transferencia de datos. La Comisión aún no ha explicado en detalle porqué las protecciones existentes contra el robo de la propiedad intelectual y el espionaje industrial son insuficientes para los flujos internacionales de datos no personales. En cualquier caso, tomar prestadas las salvaguardias de transferencia de datos desarrolladas originalmente para proteger la privacidad de las personas parece una solución engorrosa e imprecisa. La consecuencia inmediata, cuando la Ley de Datos comience a recorrer el laberinto legislativo, podría ser la preocupación exterior de que la apuesta de la UE por una mayor autonomía en la economía de los datos se dirija de nuevo en una dirección proteccionista.

VI. CONCLUSIONES

A lo largo del presente trabajo se ha puesto de manifiesto la gran transcendencia de la materia en el mundo interconectado en el que nos encontramos. Se ha analizado el régimen previsto para las transferencias internacionales de datos, tanto personales como no personales a través de un marco que pretende aunar protección y libertad de circulación. El RGPD ha unificado la normativa europea en la materia, aplicando un único sistema en lugar de las diferentes legislaciones nacionales que coexistían y reforzando la seguridad jurídica en el EEE.

En este marco, es necesario que los mecanismos establecidos salvaguarden los derechos de los interesados en el ámbito de las transferencias de datos de carácter personal como se ha puesto de manifiesto con las Sentencias Schrems I y II.

No hay que olvidar que estamos hablando del derecho fundamental a la protección de datos de carácter personal y su protección tiene que ser un objetivo común para instituciones, ciudadanos y empresas exportadoras de datos. De nada sirve garantizar un régimen de protección a los datos de carácter personal cuando en un mundo global como

[52] Veáse sobre la influencia de la UE en el mundo a través de sus políticas: Bradford, A (2020). The Brussels Effect: How the European Union Rules the World. *Oxford University Press,*

en el que nos encontramos se permite la transferencia de los mismos a países que no cumplen los requisitos exigidos por nuestra normativa común.

De esta forma, se pone de manifiesto, como se ha visto a lo largo del trabajo, la necesidad de dar cumplimiento a las garantías existentes, asegurando un nivel de protección equivalente en los países receptores de los datos de la UE.

En cuanto al marco de las transferencias de datos no personales, se ha acordado la base que regirá la materia, pero es necesario avanzar en nuevos desarrollos que faciliten el intercambio de este tipo de datos que tan vinculados se encuentran a la innovación y el desarrollo económico.

En este ámbito, la Estrategia Europea de Datos planteada por la Comisión pretende, a través de las propuestas legislativas mencionadas, promover la materia y crear un marco jurídico adecuado y que garantice las condiciones necesarias para el almacenamiento, acceso y transferencia de los datos.

No obstante, no hay que olvidar que este marco legal, se encuadra dentro de la actual regulación de la UE en la materia. En especial, el régimen de garantías previsto en el RGPD para los datos que tengan el carácter de personales. Por lo tanto, las nuevas propuestas deberán adaptarse en consonancia con el régimen de garantías que se ha analizado, sin que pueda permitirse un marco legal "paralelo" que obvie los esfuerzos realizados en el pasado.

VII. BIBLIOGRAFÍA

1. ARTÍCULOS, CAPÍTULOS DE LIBROS Y ENTRADAS DE BLOG

Bradford, A (2020). The Brussels Effect: How the European Union Rules the World. *Oxford University Press*,

Brill, J. (2016). Strengthening international ties can support increased convergence of privacy regimes. *European Data Protection Law Review nº 2*, 155-156.

Castellanos Rodríguez, A. (2017). El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio Privacy Shield. *Institut de Ciències Polítiques Socials (UAB)*, p. 12.

Cordero Álvarez, C. I. (2019). La transferencia internacional de datos con terceros Estados en el nuevo Reglamento europeo: Especial referencia al caso estadounidense y la Cloud Act. *Revista Española de Derecho Europeo*, (70), 49-108.

Christakis, T. (2020) European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy. *Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute.* http://dx.doi.org/10.2139/ssrn.3748098 (Consultado a 5 de junio de 2022).

Christakis, T. (2020) "Schrems III"? First Thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers. *European Law Blog.* https://europeanlawblog.eu/2020/11/13/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-1/ https://europeanlawblog.eu/2020/11/16/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-2/ https://europeanlawblog.eu/2020/11/17/schrems-iii-first-thoughts-on-the-edpb-post-schrems-ii-recommendations-on-international-data-transfers-part-3/ (Consultado a 5 de junio de 2022).

Gonzalo Domenech, J. J. (2019). Las decisiones de adecuación en el Derecho europeo relativas a las transferencias internacionales de datos y los mecanismos de control aplicados por los estados miembros. *Cuadernos de Derecho Transnacional*, Vol. 11, Nº 1, 350-371. https://doi.org/10.20318/cdt.2019.4624 (Consultado a 5 de junio de 2022).

IAPP-EY (2022). *Annual Privacy Governance Report 2021*. https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf (Consultado a 5 de junio de 2022).

Jarne Muñoz, P. (2019). Algunas reflexiones acerca de la propuesta de reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea. *¿Cómo poner en práctica el gobierno abierto?*, Editorial Reus, pp. 51-64.

Martín y Pérez de Nanclares, J. (2018) Comentario al artículo 8 Protección de Datos de Carácter Personal. *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo.* Fundación BBVA, 223-243 (Pág. 237). https://www.fbbva.es/wpcontent/uploads/2017/05/dat/DE_2008_carta_drechos_fundamentales.pdf (Consultado a 5 de junio de 2022).

Mantelero, A. (2021). The Future of Data Protection: Gold Standard vs. Global Standard, *Computer Law & Security Review*, vol. 40, 2021.

Polo Roca, A. (2021). Las transferencias internacionales de datos: Regulación actual y su incidencia en las relaciones exteriores de la Unión Europea. *Revista Aragonesa de Administración Pública*, (57), 325-369.

Propp K. (2022). Cultivating Euope's Data Garden. *Lawfare.* https://www.lawfareblog.com/cultivating-europes-data-garden (Consultado a 5 de junio de 2022).

Sobrino García, I. (2021). Las decisiones de adecuación en las transferencias internacionales de datos. El caso del flujo de datos entre la Unión Europea y Estados Unidos, *Revista de Derecho Comunitario Europeo*, *nº* 68, 227-256. https://www.cepc.gob.es/sites/default/files/2021-12/39318rdce6807sobrino-garcia.pdf (Consultado a 5 de junio de 2022).

Streinz, T. (2021). The Evolution of European Data Law. *The Evolution of EU Law (OUP, 3rd edn 2021)*, 902-936. https://ssrn.com/abstract=3762971 (Consultado a 5 de junio de 2022).

Uría Gavilán, E (2016). Derechos fundamentales versus vigilancia masiva. Comentario a la sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015 en el asunto C-362/14 Schrems. *Revista de Derecho Comunitario Europeo*, Año nº 20, Nº 53, 2016, 261-282.

Zalnieriute, M. (2022). Data Transfers after Schrems II: The EU-US Disagreements Over Data Privacy and National Security (April 14, 2021*). Vanderbilt Journal of Transnational Law, (2022) 55(1), pp. 1-48, UNSW Law Research.* SSRN: https://ssrn.com/abstract=3826878 (Consultado a 5 de junio de 2022).

2. FUENTES INSTITUCIONALES:

Comisión Europea. Comunicación (COM(2017) 7 final) de la Comisión al Parlamento Europeo y al Consejo relativa al Intercambio y Protección de los datos personales en un mundo globalizado.

Comisión Europea. Comunicación (COM(2019) 250 final) de la Comisión al Parlamento Europeo y al Consejo Orientaciones sobre el Reglamento relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

Comisión Europea. Comunicación (COM(2020) 66 final) de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una Estrategia Europea de Datos.

Comisión Europea. Comunicación (COM(2020) 767 final 2020/0340 (COD)) de la Comisión Europea: Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativo a la gobernanza europea de datos (Ley de Gobernanza de Datos), de 25 de noviembre de 2020.

Comisión Europea. Comunicación (COM(2020) 66 final) de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una estrategia europea de datos.

Comisión Europea: Decisiones de adecuación. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_es (Consultado a 5 de junio de 2022).

Comisión Europea: European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (Consultado a 5 de junio de 2022).

Comité Europeo de Protección de Datos. Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, adoptadas el 10 de noviembre de 2020 https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_es.pdf (Consultado a 5 de junio de 2022).

Comité Europeo de Protección de Datos: Declaración 05/2021 sobre la Ley de gobernanza de datos a la luz de la evolución legislativa, adoptada el 19 de mayo de 2021. https://edpb.europa.eu/system/files/2021-08/edpb_statementondga_19052021_es.pdf (Consultado a 5 de junio de 2022).

Comité Europeo de Protección de Datos. Statement on the Digital Services Package and Data Strategy, adopted on 18 November 2021. https://edpb.europa.eu/system/files/2021-

11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf (Consultado a 5 de junio de 2022).

Consejo de la Unión Europea (2021). Promoting data sharing: presidency reaches deal with Parliament on Data Governance Act. https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/ (Consultado a 5 de junio de 2022).

Grupo de Trabajo del Art. 29: Working Document (WP 237) 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) Adopted on 13 April 2016 https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf (Consultado a 5 de junio de 2022).

Grupo de Trabajo del Art. 29: Working Document (WP 238) Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision Adopted on 13 April 2016. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (Consultado a 5 de junio de 2022).

Grupo de Trabajo del Artículo 29: Documento de Trabajo sobre Referencias de Adecuación (WP254). Revisado 6 de febrero de 2018. https://ec.europa.eu/newsroom/article29/items/614108 (Consultado a 5 de junio de 2022).

Supervisor Europeo de Protección de Datos: *Strategy for EU institutions to comply with "Schrems II" Ruling*. https://edps.europa.eu/press-publications/press-news/press-releases/2020/strategy-eu-institutions-comply-schrems-ii-ruling_en (Consultado a 5 de junio de 2022).

The White House: FACT SHEET: United States and European Commission Announce Trans-Atlantic Data Privacy Framework. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/ (mayo de 2022) (Consultado a 5 de junio de 2022).

Tribunal de Justicia de la Unión Europea: *Ficha Temática: Protección de los Datos de Carácter Personal*. Dirección de Investigación y Documentación. (julio de 2018). https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_es.pdf (Consultado a 5 de junio de 2022).

Tribunal de Justicia de la Unión Europea: Comunicado de Prensa n º 91/20 El Tribunal de Justicia invalida la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU, https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091es.pdf (Consultado a 5 de junio de 2022).

Tribunal Europeo de Derechos Humanos: Collection of Data Protection. (enero de 2022). https://www.echr.coe.int/Documents/FS_Data_ENG.pdf (Consultado a 5 de junio de 2022).