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

ADEQUACY DECISIONS IN EUROPEAN LAW RELATED TO INTERNATIONAL DATA TRANSFERS AND CONTROL MECHANISMS APPLIED BY THE MEMBER STATES

Juan José Gonzalo Domenech
Consultor legal y seguridad
UBT Compliance

Recibido: 15.12.2018 / Aceptado: 29.01.2019
DOI: https://doi.org/10.20318/cdt.2019.4624

Resumen: La nueva legislación europea ha traído consigo un régimen sobre transferencias internacionales de datos mucho más desarrollado que la Directiva 95/46/CE, y de ello debemos destacar el nuevo régimen de la decisión de adecuación y la influencia de la STJUE Schrems en dicha redacción. El objetivo de este nuevo régimen es supervisar que todo país, sector u organización internacional declarado como "adecuado" lo continúe siendo a lo largo del tiempo, y si no fuera así, tomar medidas para resolver la situación.

Palabras clave: decisión de adecuación, RGPD, transferencia internacional de datos, Schrems.

Abstract: The new legislation has brought with it a regime on international data transfers that is much more advanced than Directive 95/46/EC, and we must highlight the new regime of the adaptation decision and the influence of RCJEU Schrems in that wording. The objective of this new regime is that the entire country, the sector or international organization declared as "adequate" continue to be so over time, and if not, take measures to fix the situation.

Keywords: adequacy decision, GDPR, international data transfer, Schrems.

I. Introducción

1. Las transferencias internacionales de datos personales han sido uno de los caballos de batalla que ha tenido que afrontar la Unión Europea en materia de protección de datos, y esto se demuestra en las constantes batallas judiciales y políticas debido la dudosa legalidad de algunos actos legislativos llevados a cabo por la Unión Europea. Podemos considerar como principales controversias propiciadas por la justicia europea los siguientes[1]:

1. La STJUE 30 de mayo de 2006, asuntos C-317/04 y C-318/04, *Parlamento vs. consejo y comisión* la nulidad de la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (EE.UU.) debido a que el tratamiento de datos objeto de la Decisión se excluye de lo estipulado por la Directiva 95/46, y de la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, oficina de aduanas y protección de fronteras, de los Estados Unidos, puesto que no puede ser adecuado a derecho la celebración de un acuerdo cuyo objeto se encuentra excluido de la directiva mencionada.
2. La Resolución del Parlamento Europeo de 23 de octubre de 2013, sobre la suspensión del acuerdo TFTP (Programa de Seguimiento de la Financiación del Terrorismo en castellano) a raíz de la vigilancia de la NSA (Agencia Nacional de Seguridad estadounidense)[2], insta a la Comisión Europea a actuar sobre la posible suspensión del acuerdo SWIFT (Sociedad para las Comunicaciones Interbancarias y Financieras Mundiales) de transmisión de datos bancaria.
3. La STJUE de la Gran Sala sobre el asunto C-362/14, *Schrems,* por el cual anula la Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro, porque se ha constatado que Estados Unidos no es un tercer país que garantice un nivel de protección adecuado.

2. Los sucesivos varapalos institucionales no han hecho más que aumentar la inseguridad jurídica dentro de los Estados miembros respecto a la posibilidad de efectuar una transferencia internacional de datos; puesto que las normas europeas vienen a traer estabilidad y uniformidad a una materia en la que se debe buscar una armonización global en los estándares de protección de datos[3]. Hasta la aplicación del RGPD, el carácter adecuado del nivel de protección era evaluado en primer lugar por el responsable del tratamiento, que transfiere datos personales a un tercer país, a veces en el marco del control a posteriori efectuado por la autoridad de control. Esta situación daba lugar a enfoques diferentes en la apreciación del nivel de protección garantizado por los terceros países u organizaciones internacionales y, por consiguiente, implicaba que el riesgo de que el nivel de protección de los interesados previsto en un tercer país se juzgue diferentemente de un Estado miembro a otro[4].

3. El objetivo primordial de estas normas es garantizar que, cuando se transfieran datos personales de ciudadanos situados en la Unión Europea a terceros países, se mantenga el mismo nivel de protección con respecto a los mismos[5].

[1] *Vid*. A. Ortega Giménez, "Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield", *Revista Lex Mercatoria: Doctrina, Praxis, Jurisprudencia y Legislación*, nº 4, 2016, p. 85.

[2] Texto aprobado, P7_TA(2013) 0449.

[3] *Vid*. F. Blas, "Transferencias internacionales de datos, perspectiva española de la necesaria búsqueda de estándares globales", *Revista Derecho del Estado*, nº 23, 2009, p. 49.

[4] COM (2010) 609.

[5] Comunicación de la Comisión al Parlamento Europeo y al Consejo. Intercambio y protección de los datos personales en un mundo globalizado. COM(2017) 7 final/2.

4. Se ha reflejado en el Reglamento (UE) 2016/679[6] (RGPD) y en la Directiva (UE) 2016/680, 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 la importancia de las transferencias de los flujos de datos a terceros países para la expansión del comercio[7] manifestado en el considerando 1 del RGPD y de la cooperación internacional en materia de seguridad y prevención de delitos en el considerando 7 de la Directiva 2016/680, pero las transferencias internacionales de datos no deben menoscabar el derecho a la protección de datos de los particulares[8]. Por ello, el nuevo régimen de las transferencias internacionales de datos del RGPD tiene una doble razón de ser: por un lado, eliminar las restricciones irracionales en el movimiento internacional de datos, y por el otro; procurar una actuación coordinada por parte de las autoridades estatales para hacer frente a la nueva delincuencia internacional. En definitiva, proporcionar garantías a todos los actores intervinientes en estas situaciones[9].

5. Las Decisiones de adecuación surgen en este nuevo contexto legal como la herramienta jurídica más "segura" para transferir datos a terceros Estados u Organizaciones Internacionales. Tras la derogación de la Decisión de los principios de Safe Harbour, dichas Decisiones se encuentran en tela de juicio a raíz de la STJUE *Schrems* en 2015. De hecho, ya la propia Comisión consideraba que estas Decisiones no estaban lo suficientemente especificadas[10], por lo podría producir inseguridad en los actores en los movimientos internacionales de datos.

II. Concepto sobre Transferencia internacional de datos

6. El concepto objeto de estudio debe entenderse desde una doble perspectiva del Derecho europeo y el Derecho internacional emanado del Convenio del Consejo de Europa 108, relativo a la protección de los individuos en el tratamiento automatizado de datos personales, actualizado por el protocolo 223 (Convenio 108+). La determinación de dicho concepto desde una perspectiva técnica se antoja difícil en la práctica debido a los numerosos medios electrónicos e intermediarios que nos podemos encontrar en el proceso[11], pero legalmente, la definición de "transferencia internacional de datos" podemos encontrarla en el Informe explicativo del artículo 14 del Convenio 108+ definiéndola como aquellos datos personales se divulgan o se ponen a disposición de un receptor sujeto a la jurisdicción de otro Estado u organización internacional[12]. La definición presentada por el texto deriva de una construcción doctrinal y jurisprudencial[13] empezando por el TJUE, sin llegar a dar una definición formal, ha delimitado en sentido negativo el contenido de la definición a raíz de la STJUE *Lindqvist*[14].

7. El objeto principal de la cuestión planteada al TJUE era determinar si la publicación de datos personales en una página web almacenada por su proveedor de servicios de alojamiento domiciliado en la Unión, en la que se puede acceder desde cualquier lugar debe ser considerada como una transferencia

[6] DOUE L 119/1, de 4 de mayo de 2016.

[7] *Vid*. J. Oster, *European and International Media Law*, Cambridge (UK), Cambridge University Press, 2017, p. 351.

[8] *Vid*. Considerando 101 del RGPD, y 69 y 70 de la Directiva 680/2016.

[9] *Vid*. M. Recio Gayo, *Protección de datos personales e innovación: ¿(In)compatibles?*, Madrid, Reus, 2016, p. 89.

[10] COM (2010) 609 final.

[11] *Vid*. W. Kuan Hon, *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*, Cheltenham, Edward Elgar Publishing, 2017, p. 69.

[12] *A transborder data transfer occurs when personal data is disclosed or made available to a recipient subject to the jurisdiction of another State or international organisation.*

[13] El Real decreto 1720/2007 que desarrolla la LO 15/1999 recogía una definición en el Artículo 5.1.s): Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

[14] STJUE 6 de noviembre de 2003, *Lindqvist*, C-101-01.

internacional (apartado 71 STJUE *Lindqvist*), la cual se determinó que no debe considerarse como tal; aunque sí se considera un tratamiento de datos[15].

8. El tribunal basa su fallo fundamentalmente en la naturaleza técnica de las operaciones efectuadas. El acto de haber publicado en una página web los datos personales no implica *una transmisión directa entre dos sujetos, sino que se han transmitido con ayuda de una infraestructura informática* (apartado 60 STJUE *Lindqvist*). Esto quiere decir que uno de los elementos constituyentes de una "transferencia internacional de datos" es la existencia de dos sujetos en el proceso (un exportador de datos, y un importador de estos).

9. Siguiendo (en parte) a la doctrina, una "transferencia internacional de datos" deberá constar de los siguientes elementos[16]:

1) Debe tratarse de datos de carácter personal; esto es, de "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables". En definitiva; "que permitan identificar o hacer identificable a una persona de manera directa o indirecta"[17].
2) Los datos de carácter personal que vayan a transmitirse vienen referidos tanto a aquellos que son tratados de forma automatizada (movimientos realizados por medios informatizados) como a los tratados de forma no automatizada (aquellos realizados por medios convencionales).
3) La transferencia internacional de datos se efectúa con el objeto de realizar un tratamiento de datos de carácter personal por parte del destinatario de los mismos, ya sea tanto cesión (a otro responsable) como prestación de un servicio (encargado de tratamiento).
4) El traslado físico efectivo de los datos de carácter personal, de un lugar del EEE a cualquier otro Estado, región, u Organización Internacional.
5) El lugar de destino de los datos de carácter personal debe encontrarse en un territorio externo al EEE o de las partes no contratantes.
6) Existirá transferencia internacional de datos personales en cualquiera de los dos casos siguientes: cuando constituya una cesión o comunicación de datos o cuando tenga por objeto la realización de un tratamiento de datos por cuenta del responsable mediante un encargo de tratamiento.

10. Como hemos visto, supone un movimiento de datos entre un exportador, y un importador, los cuales pueden actuar como responsables o encargados; por lo que, dependiendo de la posición de las partes en esta operación, el exportador deberá cumplir con el deber de información, legitimar la transferencia mediante la base legal o excepción contemplada, y la adopción de un acto vinculante que contenga las disposiciones del artículo 28 del RGPD, y cualesquiera otras obligaciones que imponga la legislación nacional en caso de que nos encontremos ante un movimiento de responsable a encargado, o un contrato de cesión donde se presten las garantías adecuadas.

11. Nadie duda de los supuestos de acceso internacional a bases de datos mediante instrumentos remotos[18], e incluso se ha llegado a valorar la posibilidad de considerar los supuestos de "acceso internacional" a páginas webs como transferencias internacionales. PIÑAR MAÑAS aporta como argumento el nuevo artículo 49.1.g) del RGPD, que considera válida la transferencia cuando se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar la información al público y esté abierto a la consulta del público en general o de cualquier persona que

[15] Apartado 27 STJUE *Lindqvist*.

[16] *Vid*. Ortega Giménez, A., *La (des) protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, AEPD, Madrid, 2015, pp. 23, y *Transferencias internacionales de datos de carácter personal ilícitas*, Cizur Menor, Aranzadi, 2017, p. 31.

[17] *Vid*. Artículo 4.1) del RGPD.

[18] *Vid.* Informe AEPD 190/2007.

pueda acreditar un interés, pero solo en la medida en el que se cumplan las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta. Es decir, bastaría con la puesta a disposición de los datos[19], misma postura que mantiene el Supervisor Europeo de Protección de Datos[20]. Aunque puede llegar a asimilarse, es dudosa la analogía presentada al asemejar un registro oficial de cualquier Estado miembro a cualquier página web de internet observando la literalidad de la norma.

III. El principio general de las transferencias internacionales de datos personales y las decisiones de adecuación

1. El principio general de las transferencias internacionales de datos

12. El principio contemplado en la normativa de aplicación[21] determina que solo se podrán efectuar transferencias internacionales de datos a un tercer país u organización internacional si: 1) cumple con todas las obligaciones relativas al tratamiento recogidas en la normativa aplicable (muy complicado en la práctica), 2) asegura las suficientes garantías a la hora de realizar la transferencia internacional, en especial, las consistentes en garantías en las ulteriores transferencias. Por lo tanto, si un responsable pretende transferir datos personales a un tercer Estado, región u organización internacional no solo debe afirmar que es "segura", también debe acreditar que cumple con todos los elementos obligatorios y que, en caso de efectuar sucesivas transferencias internacionales de datos a otros proveedores, también estos adoptan las garantías tecnológicas suficientes[22]. En efecto, este método supone un sistema de "doble factor"[23] en el que se deben cumplir escalonadamente dichos criterios para efectuar una transferencia.

13. Por otra parte, el Convenio 108+ impone la regla general del libre movimiento de datos entre las partes contratantes del Convenio, sin que se admitiese ninguna prohibición a este libre movimiento, más que la existencia de un riesgo en el Estado contratante sobre el incumplimiento de las disposiciones del tratado. Pero la presente disposición limita su aplicación en los Estados contratantes que tuviesen normas armonizadas sobre transferencias internacionales de datos personales. Es decir, un Estado de la Unión Europea no podrá enviar libremente los datos personales a un Estado contratante no miembro de la Unión, teniendo que cumplir el Estado exportador las obligaciones de la normativa europea, con el fin de proteger bajo las leyes de la Unión Europea el movimiento internacional de datos de los habitantes de la Unión Europea[24].

14. En el caso de la Directiva 2016/680, se establecen principios completamente opuestos con el fin de adaptar el fin de la transferencia al objeto de la Directiva. Se establece un principio general de prohibición de realizar transferencias internacionales, salvo que se cumplan una serie de requisitos:

a) El fin de la transferencia debe ser la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública.
b) La transferencia debe hacerse a una autoridad competente como responsable del tratamiento cuya misión sea similar al fin de la transferencia.
c) Si los datos fueran obtenidos de otro Estado miembro, será necesario el consentimiento de dicho Estado para la transferencia.

[19] *Vid.* J. L. Piñar Mañas, *op. cit*., p. 433.
[20] *Vid*. SEPD, The transfer of personal data to third countries and international organizations by EU institutions and bodies, Position paper, Bruselas, 2014, pp. 5-6.
[21] Artículos 44 del RGPD, 36 de la Directiva 206/680 y 14 del Convenio 108+.
[22] *Vid*. E. Díaz Díaz, "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones", *Revista Aranzadi Doctrinal*, núm. 6, 2016, p. 13.
[23] *Vid*. A. Paul Voigt, von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017, pp. 117.
[24] *Vid.* European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law*, Luxemburgo, Oficina de la Unión Europea, 2018, p. 52.

d) Las garantías adecuadas, que pueden plasmarse mediante una Decisión de la Comisión, o mediante otros instrumentos jurídicos vinculantes, y
e) En caso de transferencias ulteriores, la debida ponderación por la autoridad de control pertinente entre el riesgo que supone la transferencia y la gravedad del delito perseguido.

2. Concepto y características de la Decisión de Adecuación

15. Como norma general, esa transferencia será autorizada mediante una decisión de adecuación que certifique que ese país, región, u organización internacional tiene un "nivel de protección adecuado" sin necesidad de autorización singular de alguna Autoridad de Supervisión. Una decisión de adecuación no deja de ser una Decisión de Ejecución, un acto jurídico realizado por la Comisión Europea y habilitado en este caso por el RGPD, Directiva 2016/680 y el artículo 288 del TFUE que permite declarar a un tercer Estado con un nivel de protección adecuado. La decisión no viene a declarar la legislación sobre protección de datos de ese tercer Estado "igual" que el reglamento, sino que viene a valorar adecuadamente la legislación, o en términos de la STJUE *Schrems*, declarar la legislación del tercer Estado "sustancialmente equivalente"[25]. Para lograrlo, "los medios a los que puede recurrir un tercer país, a este respecto, a los efectos de dicho nivel de protección pueden diferir de los empleados en la UE". Por lo tanto, el objetivo no es reflejar punto por punto la legislación europea, sino establecer los requisitos básicos esenciales de esa legislación.

16. Como acto jurídico vinculante de la Unión Europea, tiene eficacia directa en los Estados miembros, y viene a informar a dichos Estados que se pueden realizar transferencias internacionales a esos terceros Estados sin ninguna restricción. Por lo tanto, podemos considerar este instrumento como el medio más eficaz para la realización de transferencias internacionales a terceros Estados debido a su generalidad y "confianza" que aporta la Comisión Europea al garantizar como seguro a ese tercer Estado, aunque debe tomarse al fin y al cabo como una presunción de garantía, tal y como hemos observado en la STJUE *Schrems*, puesto que podría impugnarse ante el TJUE dicha Decisión si se constatase que el tercer Estado, región u organización internacional no garantiza un nivel de seguridad suficiente.

17. Una característica reseñable de las Decisiones de adecuación es la flexibilidad con la que se pueden configurar de cara a las condiciones de transmisión con esos terceros sujetos. Las Decisiones de adecuación pueden referirse tanto a una adecuación "total" del territorio o a una adecuación parcial; es el caso de las Decisiones de adecuación sobre Canadá y Estados tratan sobre adecuaciones parciales a determinados sectores o empresas. En Canadá, solo podrán transferirse datos personales a las entidades que se enmarquen en la *Personal Information Protection and Electronic Documents Act*; y en EE. UU, a las entidades que hayan adquirido unos estándares y principios relativos a la protección de datos, o incluso para determinados tratamientos, como es Israel, que se aplica para los tratamientos automatizados.

18. El efecto principal de una decisión de adecuación es la innecesidad de una autorización específica (artículo 45.1 del RGPD) al otorgar una equivalencia de la transferencia realizada a ese tercer Estado u organización internacional a un movimiento de datos realizado entre los Estados del Espacio Económico Europeo, aunque no supone en ningún momento la excepción de cumplir con la adopción de un contrato de encargado entre el exportador y el importador y, aunque no fuese obligatorio en las comunicaciones de datos personales, un contrato de cesión de datos donde estipule una serie de garantías respecto al origen y base legal de la recogida de datos permitiría afrontar estas operaciones con mayor seguridad jurídica tanto para las partes como para los afectados. Cabe decir que el hecho de que se haya emitido una decisión de adecuación sobre la base del RGPD, no equivale a obtener un reconocimiento similar respecto a las decisiones de adecuación sobre la base de la Directiva 2016/680 a tenor del

[25] STJUE 6 de octubre de 2015, *Maximillian Schrems / Data Protection Commissioner*, C-362/14, apartados 73, 74 y 96. Véanse también el considerando 104 del RGPD y el considerando 67 de la Directiva 680/2016.

considerando 68 de esta norma, por lo que serán necesarias decisiones de adecuación separadas, o una decisión que, expresamente, reconozca el alcance de la decisión a los fines del RGPD y de la Directiva 680/2016; aunque la Comisión Europea deberá tener en cuenta las decisiones de adecuación realizadas sobre la base del RGPD. Consecuentemente la adopción de una Decisión de adecuación conlleva también un deber de supervisión de para la Comisión Europea de manera continuada de los acontecimientos de dichos países, sectores u organizaciones internacionales (artículo 45.4 del RGPD).

19. El 8 de febrero de 2018, el Grupo de trabajo del artículo 29 (que a partir del 25 de mayo pasó a denominarse Comité Europeo de Protección de Datos) publicó el WP254, una actualización del WP12 por el cual estipula y enumera unos requisitos respecto a la consideración como "adecuado" el nivel de protección de un Estado, el cual era de 1998[26]. El nuevo WP viene a desarrollar los requisitos recogidos en el artículo 45 del RGPD. La consideración de "adecuado" se logra mediante una combinación de derechos para los afectados y obligaciones para los responsables del tratamiento y qué tipo de organismo puede hacer cumplir los derechos, y sobre todo el sistema que garantice la efectividad de la legislación vigente. Este concepto ha sido criticado por su ambigüedad, por lo que la existencia de este documento viene a arrojar claridad respecto a la interpretación y conceptualización de dicho requisito[27]

3. Criterios de valoración para determinar la Decisión de Adecuación

20. Este tipo de decisiones rompen el procedimiento tradicional de las decisiones europeas, por lo que se ha instaurado un procedimiento donde intervienen más actores y criterios a la hora de redactar la Decisión, lo que supone un procedimiento especial adecuado a las necesidades propias de la legislación de protección de datos, que goza de una sensibilidad especial.

21. Los elementos, principios y condiciones que se tienen en cuenta para determinar a un tercer Estado, región u organización internacional como seguro se encuentran en varios documentos tanto normativos como recomendaciones de diferentes organismos de la Unión Europea.

A) Prerrequisitos

22. En primer lugar, la Comisión Europea ha adoptado en la Comunicación al Parlamento Europeo y al Consejo sobre Intercambio y protección de los datos personales en un mundo globalizado, una serie de criterios por los cuales sirven como punto de partida a la hora de entablar un diálogo para decidir sobre la adecuación:

a) el alcance de las relaciones comerciales (efectivas o posibles) de la UE con un determinado tercer país, incluida la existencia de un acuerdo de libre comercio o de negociaciones en curso;
b) la magnitud de los flujos de datos personales con origen en la UE, que reflejan lazos geográficos o culturales;
c) 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, y
d) 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.

23. Estos prerrequisitos tienen una finalidad comercial con dichos países, y se priorizarán a aquellos que, por intereses comerciales, se precise la necesidad de establecer una Decisión de adecua-

[26] WP12, "Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive" adoptado por el Working Part el 24 de julio de 1998.

[27] *Vid*. E. Cerda Silva, "El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea, *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, núm. 36, 2011, p. 335.

ción para aumentar las relaciones con dichos sujetos. Los dos últimos prerrequisitos suponen examinar de forma superficial los criterios recogidos en la norma, lo que supone prejuzgar el cumplimiento de los requisitos antes de hacerlo en su fase correspondiente.

B) Condiciones del artículo 45 del RGPD y 36 de la Directiva 2016/680: principios y *enforcement*

24. Una vez constatados los prerrequisitos para comenzar el diálogo con los Estados, regiones u organizaciones internacionales, se valorarán los requisitos propios del artículo 45 del RGPD:

a) El marco jurídico en general: el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional;
a) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los afectados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
c) 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, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

25. Por lo tanto, es evidente que cualquier análisis significativo de la protección adecuada debe comprender los dos elementos básicos: 1) el contenido de las normas aplicables y 2) los medios para garantizar su aplicación efectiva. Corresponde a la Comisión Europea verificar, de forma periódica, que las normas establecidas sean efectivas en la práctica. Ese contenido debe tener como "modelo a seguir" las reglas contenidas en la Carta de Derechos Fundamentales de la Unión Europea y el propio RGPD, además de la propia participación del Estado en convenios internacionales tales como el Convenio 108 o la participación en otros estándares internacionales como las *Guidelines for the Regulation of Computerized Personal Data Files*. Aprobadas por la Asamblea General en su resolución 45/95 (1990); Marco de privacidad del Foro de Cooperación Económica Asia Pacífico (2005); Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana; Estándares internacionales de Privacidad. Resolución de Madrid (noviembre 2009) y las Directrices de privacidad de la Organización para la Cooperación y el Desarrollo Económicos (2013). Ya adelantamos que el cumplimiento de dichos principios se prevén difíciles de cumplir por las organizaciones internacionales, puesto a que están fuertemente orientados a los Estados.

26. El contenido de los principios relativos a la protección de datos se ha manifestado en el WP254. Todos ellos suponen en síntesis los elementos fundamentales plasmados en el RGPD, y que deberían estar en toda legislación para que pueda considerarse como "equivalente" a efectos de la Comisión Europea. En general, este conjunto de requisitos viene a modernizar los ya recogidos en el WP12, adaptándolos tanto a la actual legislación como a la situación global respecto a la protección de datos:

a) Conceptos: no significa que deban ser iguales a los recogidos en el RGPD, pero que reflejen su significado a la luz del reglamento.
b) Bases legales: Los datos deben procesarse de manera legal, justa y legítima. Las bases legales deben ser lo suficientemente claras. Algunos ejemplos pueden ser las disposiciones de

la legislación nacional, el consentimiento del interesado, la ejecución de un contrato o un interés legítimo del responsable del tratamiento o de un tercero que no anula los intereses del individuo.

c) Principio de limitación del tratamiento: tratar los datos solo para la finalidad prevista y limitar los tratamientos ulteriores para finalidades compatibles entre sí.
d) Principios de calidad de los datos y el de proporcionalidad: Los datos deben ser precisos y, de ser necesario, mantenerse actualizados. Los datos deben ser adecuados, relevantes y no excesivos en relación con los fines para los que se tratan.
e) Conservación de datos: como regla general, no se deben guardar por más de lo necesario de acuerdo a la finalidad.
f) Principios de seguridad y confidencialidad: durante el proceso de tratamiento debe aplicarse los principios de privacidad desde el diseño y por defecto para defenderse de cualquier amenaza.
g) Principio de transparencia: la información para los afectados debe transmitirse de forma clara, accesible, concisa, transparente e inteligible.
h) Derechos de acceso, rectificación, supresión y oposición: Deben contemplarse en la legislación extranjera el núcleo duro de los derechos de la protección de datos; con el límite a esos derechos la salvaguarda de las investigaciones penales, la seguridad nacional, la independencia judicial y los procedimientos judiciales u otros objetivos importantes de interés público general.
i) Restricciones en las transferencias posteriores: las transferencias posteriores deben limitarse. Solo se podrán realizar cuando el país posterior garantice un nivel de protección al del primer país destinatario.

27. En determinados tratamientos que puedan afectar de manera más sensible a los sujetos, deberán contener las siguientes previsiones con un fin más protector:

a) Datos especialmente protegidos: para dicha categoría de datos, es necesaria una base legal más reforzada, como puede ser el consentimiento explícito.
b) Marketing directo: cuando esta sea la finalidad, el afectado deberá tener el derecho a oponerse a dicho tratamiento en cualquier momento.
c) Decisiones automatizadas y *profiling*: deben existir ciertas condiciones para aplicar dicho tratamiento, como puede ser la existencia del consentimiento del afectado o la necesidad para la ejecución de un contrato, además de las salvaguardas necesarias como el derecho a ser informado sobre los motivos específicos subyacentes a la decisión y la lógica involucrada, para corregir información inexacta o incompleta, y para impugnar la decisión donde ha sido adoptado sobre una base fáctica incorrecta.

28. El conjunto anterior de previsiones no deja de ser un contenido "principial" sobre lo que una legislación sobre protección de estos debería ser, pero ese contenido carecerá de valor práctico sin un sistema de aplicación y cumplimiento de dicho contenido. El *enforcement* se erige como pilar fundamental en cualquier Estado que desarrolle el derecho a la protección de datos, y el Comité Europeo de Protección de Datos (CEPD) presenta las medidas para aplicar este concepto:

a) Autoridad de supervisión independiente: en el tercer Estado debe existir una autoridad independiente que supervise el cumplimiento de la legislación sobre la protección de datos y que tenga facultades inspectoras.
b) La legislación sobre protección de datos debe garantizar el cumplimiento: debe establecerse un sistema de obligaciones y responsabilidades, y para los interesados en concreto, debe existir un marco de derechos y medios para ejercerlos. A su vez, debe existir también un conjunto de sanciones disuasorias.
c) Cumplimiento por parte de los actores: Las entidades que traten datos personales deben poder probar el cumplimiento de la normativa ante la autoridad de supervisión independiente.

Las medidas pueden ser, por ejemplo, evaluaciones de impacto de protección de datos, mantenimiento de registros o archivos de registro de actividades de tratamiento de datos durante un período de tiempo apropiado, la designación de un Delegado de Protección de Datos, o incluir en los procesos medidas de protección de datos por diseño y por defecto.

d) La legislación sobre protección de datos debe orientarse al apoyo y ayuda de los afectados en el ejercicio de sus derechos: Deben existir mecanismos legales para el efectivo cumplimiento de los derechos de los afectados como un sistema de denuncias ante la autoridad independiente sin que su acceso suponga un coste prohibitivo al afectado, además de otros medios legales que permitan tener una indemnización en el caso de que se haya producido un daño efectivo y un sistema de sanciones efectivas.

C) Condiciones del tratamiento de los datos personales por parte de los Estados

29. Otro criterio a tener en cuenta es el marco legal de los supuestos de acceso a datos personales que realizan los propios Estados, como son los WP 237 sobre videovigilancia y WP 228 sobre vigilancia en las comunicaciones electrónicas para fines de inteligencia y seguridad nacional. Ahora más que nunca, los Estados están orientando su política de seguridad nacional para permitir el acceso a datos personales en caso de que pueda invocar este motivo debido a las condiciones sociopolíticas que sufrimos actualmente, por lo que debe considerarse este marco a la hora de determinar la adecuación de un Estado. Para considerar como un Estado con garantías, deberán cumplirse los siguientes principios:

1) El tratamiento debe basarse en reglas claras, precisas y accesibles (base legal).
2) Es necesario demostrar la necesidad y la proporcionalidad con respecto a los objetivos legítimos perseguidos.
3) El procesamiento debe estar sujeto a supervisión independiente.
4) Deben ponerse a disposición de los afectados acciones efectivas.

30. En este sentido, los terceros Estados deberán conseguir unas garantías equivalentes a las ofrecidas por la Directiva 2016/680, puesto que esta norma contempla unas limitaciones al derecho fundamental a la protección de datos asumibles a los intereses públicos que persiguen los Estados en materia de prevención delictiva.

4. Cuestiones procedimentales de la Decisión de adecuación

31. El procedimiento para instar una decisión de adecuación no se recoge en el RGPD, pero podemos vislumbrar a algunos actores que pueden instarlo[28]:

a) La propia Comisión Europea, previa valoración de los prerrequisitos mencionados.
b) El Comité Europeo de Protección de datos, cuyo artículo 70.1 permite actuar por iniciativa propia en el ejercicio de sus funciones, que alcanza al dictamen de la letra s).
c) Por un Acuerdo Internacional previo suscrito por la Comisión, como fue el caso del Acuerdo entre la Comisión Europea y EE. UU de 2 de febrero de 2016, que dio lugar a la aprobación del *Privacy Shield*, o el más recientemente, el Tratado de Libre Comercio firmado con Japón.
d) Por instancia del propio sujeto interesado y supeditado a los prerrequisitos de la propia Comisión.

32. Si la Comisión valora que el tercer país, organización internacional o sector cumple todos los principios y requisitos legales, la Comisión Europea emitirá un acto de ejecución (Decisión) declarando a ese tercer país, organización o región como seguro. En la propia Decisión deberá estipularse

[28] *Vid*. J. L. Piñar Mañas, "Transferencias de datos personales a terceros países u organizaciones internacionales", en J. L. Piñar Mañas, (Dir.), *op. cit.*, p. 441.

el ámbito de aplicación territorial y sectorial y las autoridades independientes. Deberá emitirse previamente la opinión del Comité Europeo de Protección de Datos evaluando el nivel de seguridad de dicha entidad. La decisión se tomará conforme al artículo 5 del Reglamento (UE) 2011/182 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[29].

33. Podemos encontrar un sistema de triple control tanto *ex ante* como *ex post* a la hora de dictar una Decisión de adecuación. Este sistema garantiza, por un lado, la compatibilidad previa con el Derecho de la Unión tanto de forma general como especial en cuanto a la protección de datos; y por el otro, garantizar la adecuación posterior de la Decisión a la realidad jurídico-social del momento:

34. Un primer control *ex ante* de carácter general del procedimiento de examen. Antes de aprobar cualquier acto de ejecución, el proyecto debe ser sometido al dictamen de un comité de representantes de los miembros de la Unión Europea (como el del artículo 31 de la Directiva 95/46CE, el cual viene a ser sustituido), pero bajo el régimen del procedimiento de examen del Reglamento (UE) 2011/182, mediante la adopción del dictamen por las mayorías del artículo 238.3 del TFUE al tratarse de un proyecto de decisión de la Comisión Europea. Los porcentajes de votación son:

i. Si una mayoría cualificada (el 55% de los países de la UE que representen como mínimo al 65% de la población total de la UE) vota a favor de la propuesta de acto de ejecución, la Comisión debe adoptarlo.
ii. Si una mayoría cualificada vota en contra de la propuesta, la Comisión no puede adoptarlo. En este caso, la Comisión puede recurrir a comité de apelación.
iii. Si no hay mayoría cualificada ni a favor ni en contra del acto propuesto, la Comisión puede adoptarlo o presentar una nueva versión modificada.

35. Esta metodología, bautizada como "comitología" supone una herramienta de control a la Comisión Europea por parte de los miembros de la Unión Europea, y se refleja en el dictamen vinculante de dicho Comité, el cual, si no aprueba el proyecto, la decisión no sale aprobada.

36. Un segundo control *ex ante* de carácter específico. A su vez, el artículo 70.1.s) del RGPD habilita al Comité Europeo de Protección de Datos a emitir un dictamen sobre la adecuación de ese tercer Estado, región u organización internacional; para ello le será remitida toda la información pertinente tales como la correspondencia con ese destinatario, que es de obligada redacción según el Considerando 105 del RGPD. El ejemplo más reciente lo encontramos en la correspondencia mantenida con el gobierno de los EE.UU. Hay que destacar que la opinión que dicte el Comité Europeo de Protección de Datos no es vinculante, a diferencia del dictamen del comité del Reglamento (UE) 184/2011. Sin embargo, en la práctica se ve la necesidad de coincidencia de ambas opiniones. Se ve improbable que el comité de representantes, erigido como órgano de control de la Comisión Europea en primera instancia apruebe un proyecto de decisión el cual no cuenta con el beneplácito del Comité Europeo de Protección de Datos. Este control ejercido por el comité presenta un carácter más técnico que en el recogido en el procedimiento de examen, puesto que el primero mientas analiza la compatibilidad con el Derecho de la Unión en general, este segundo presta atención a la compatibilidad con la protección de dato.

37. Un tercer control *ex post* por la propia Comisión Europea. Una vez ya sea de aplicación la Decisión, se prevé un mecanismo de revisión cada cuatro años con el objetivo de controlar si ese tercer estado, región, u organización internacional sigue cumpliendo con tales condiciones (45.3 RGPD). Si se observa que ya no se cumple tal nivel, la Comisión derogará, suspenderá o modificará la decisión y

[29] DOUE L 55/13 de 28.2.2011. Actualmente hay una propuesta de reforma: Propuesta de Reglamento Del Parlamento Europeo y del Consejo que modifica el Reglamento (UE) n.º 182/2011, 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 (COM(2017) 85 final).

para ello, según el Considerando 106, deberá tener en cuenta los pronunciamientos del Parlamento y Consejo, además de la opinión de otras entidades. La decisión que estipule que ya no se garantiza un nivel adecuado de protección, tendrá como efecto directo la prohibición de realizar transferencias internacionales de datos (Considerando 107 del RGPD), sin perjuicio de las transferencias realizadas con los mecanismos de los arts. 46-49 del RGPD. Se entablarán conversaciones con ese estado para poner remedio a la situación anterior (45.6 RGPD). Esta última previsión hace una clara referencia a la STJUE *Schrems*, por la cual se anuló a Decisión 2000/520. Aunque según el WP 254, ese marco de cuatro años debe adaptarse según el tercer Estado al que se refiera la Decisión de Adecuación debido a la estabilidad del propio Estado en el marco de la legislación sobre protección de datos: si dicho Estado emprende una reforma, será necesaria la revisión de esta nueva legislación, lo que adelantaría la misma.

38. Sin embargo, encontramos un hito procedimental no previsto en la norma tras la aprobación de la Decisión de ejecución de 23 de enero de 2019[30] por la que declara adecuadas las garantías ofrecidas por Japón. Observamos en el Considerando 190 que el Parlamento Europeo emitió una resolución sobre la idoneidad de las garantías ofrecidas por Japón respecto a la protección de datos[31] promovida por el Comité de Libertades, Justicia y asuntos interiores. El Parlamento Europeo avaló el proyecto de decisión, siendo el último paso previo a su adopción. La participación de este órgano, sin duda, refuerza aún más el acto emitido por la Comisión al contar con otro de los principales órganos políticos de la Unión Europea, y que esperemos sea continuada su participación en futuros procedimientos.

39. El artículo 45.9 del RGPD determina que las actuales decisiones de adecuación continuarán vigentes hasta que la Comisión Europea las modifique o anule Actualmente; los Estados sobre los que existe una decisión de adecuación son: Suiza[32], Canadá[33], Argentina[34], Guernsey[35], Isla de Man[36], Jersey[37], Islas Feroe[38], Andorra[39], Israel[40], Uruguay[41], Nueva Zelanda[42], y Estados Unidos de América[43]. Estas decisiones deben revaluarse hasta el 25 de mayo de 2020 y a partir de ahí, cada cuatro años como mínimo. Actualmente se mantienen conversaciones con Corea del Sur[44] y se tienen en cuenta a otros socios estratégicos como la India, países de América Latina y países con la vecindad europea.

IV. Las modificaciones urgentes llevadas a cabo por la Decisión de ejecución 2016/2295 de la Comisión, de 16 de diciembre de 2016 derivadas de la STJUE *Schrems*

40. Las decisiones de todos estos Estados –excepto la de EE.UU. y Canadá– fueron modificadas por la Decisión de ejecución 2016/2295 de la Comisión, de 16 de diciembre de 2016; en las que se añadieron mayores controles por parte de la Comisión a los países con el nivel de protección adecuado respecto a su ordenamientos jurídicos.

[30] C(2019) 304 final.
[31] 2018/2979(RSP).
[32] Decisión 2000/518/CE de la Comisión, de 26 de julio.
[33] Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos.
[34] Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
[35] Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
[36] Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.
[37] Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
[38] Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
[39] Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
[40] Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
[41] Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
[42] Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.
[43] Decisión 2016/1250 de la Comisión, de 12 de julio de 2016. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE. UU.
[44] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

41. La modificación perseguía un fin claro: evitar otro caso *Schrems*. Analizando detenidamente la STJUE, el tribunal se basa en dos pilares fundamentales para decretar la nulidad de la decisión 2000/520:

a) La nulidad del artículo 1 de la Decisión: Dicho artículo garantizaba que los principios de puerto seguro recogidos en el anexo I de la Decisión. En lo propios principios se estipula una primacía de las exigencias de seguridad nacional, interés público y cumplimiento de la ley estadounidense sobre los propios principios, por lo que se permite una injerencia en sus derechos fundamentales con la mera alegación de dichas razones. A su vez, no existen normas en EE.UU que limite las injerencias en la vida privada de las personas, y loa mecanismos de resolución de conflictos solo afectan a conflictos entre afectados y empresas, no cuando la injerencia se produzca por parte del Estado. Además, la ley estadounidense no establece límites a la conservación y tratamientos de datos personales transferidos desde la Unión Europea a EE.UU y que por motivos similares, el TJUE declaró nula la Directiva 2006/24/CE en la STJUE *Digital Rights Ireland*. Visto que EE.UU no garantiza un adecuado nivel de protección, dicho artículo contradice a los arts. 7 y 8 de la Carta Europea de Derechos Fundamentales.
b) La nulidad del artículo 3[45] de la Decisión: Cuestión que pretendo resaltar en el presente apartado, dicho artículo fue declarado también nulo. El artículo 28.6 de la Directiva permite a cualquier autoridad de control de los Estados miembros ejercer con independencia cualquier competencia atribuida por la propia Directiva. En este caso, la autoridad de control sería competente para resolver cualquier solicitud relativa a la compatibilidad de una decisión de la Comisión Europea con la propia Directiva en virtud de las competencias también atribuidas por los Estados miembros[46]. Pero la decisión estipulaba un régimen limitativo de las competencias de las autoridades de control que contradecía al artículo 28 de la Directiva 95/46/CE.

[45] Artículo 3 de las Decisiones de adecuación previas a la reforma por la Decisión de ejecución 2295/2016: *1. Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos siguientes:*

a) el organismo público de Estados Unidos de América contemplado en el anexo VII de la presente Decisión, o un [órgano] independiente de recurso, a efectos de la letra a) del principio de aplicación, que figura en el anexo I de la presente Decisión, ha resuelto que la entidad ha vulnerado los principios y su aplicación de conformidad con las FAQ; o

b) existen grandes probabilidades de que se estén vulnerando los principios; existen razones para creer que el [órgano] de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad y proporcionarle la oportunidad de alegar.

La suspensión cesará en cuanto esté garantizado el cumplimiento de los principios y su aplicación de conformidad con las FAQ y las autoridades correspondientes de la Unión Europea hayan sido notificadas de ello.

2. Los Estados miembros informarán a la Comisión a la mayor brevedad de la adopción de medidas con arreglo al apartado 1.

3. Asimismo, los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no garantice dicho cumplimiento.

4. Si la información recogida con arreglo a los apartados 1 a 3 demuestra que un organismo responsable del cumplimiento de los principios y su aplicación de conformidad con las FAQ en Estados Unidos de América no está ejerciendo su función, la Comisión lo notificará al Departamento de Comercio de Estados Unidos de América y, si procede, presentará un proyecto de medidas con arreglo al procedimiento que establece el artículo 31 de la Directiva, a fin de anular o suspender la presente Decisión o limitar su ámbito de aplicación.

[46] El TJUE (SSTJUE 22 de octubre de 1987, *Foto-Frost*, 314/85 y 10 de enero de 2006, *IATA y ELFAA*, C-344/04) ya consideró que los órganos judiciales y administrativos de cualquier Estado miembro no pueden declarar la invalidez de cualquier acto de las instituciones europeas, pero permiten a los Estados miembros habilitar mecanismos para que dichos órganos (en este caso, la AEPD) puedan alzar un recurso ante el propio TJUE, mecanismo jurídico que no existe en nuestro ordenamiento, pero con el nuevo artículo 58.5 del RGPD, faculta a las autoridades de control para poner en conocimiento de las autoridades judiciales el incumplimiento del Reglamento.

42. Este motivo no trascendería más allá de la presente Decisión, pero la sentencia podría llegar a alcanzar a las demás Decisiones de adecuación, puesto que el mismo contenido de esta Decisión se repetía en las demás, y eran susceptibles de poder ser invalidadas.

43. De ahí el ser de la Decisión de ejecución 2016/2295, cuyo contenido viene a modificar transversalmente y por igual a todas decisiones mediante una nueva redacción al artículo 3[47] de cada una de ellas, que elimina las restricciones que pesaban sobre las autoridades de control y establece una obligación para la Comisión consistente en la supervisión continua tanto de la legislación como de los acontecimientos en dicho país y cómo es la evolución de las normas que permiten el acceso a los datos personales a las autoridades.

V. La Decisión 2016/1250 y las dudas sobre su validez

1. Características generales

44. Debido a la derogación de la Decisión 2000/520, y a raíz del acuerdo entre la Comisión Europea y EE. UU., fue aprobada la Decisión de ejecución 2016/1250 el 12 de julio y de aplicación el 1 de agosto[48] a raíz del acuerdo firmado entre la Comisión Europea y EE.UU previamente mencionado. La estructura de la nueva Decisión consta de solo seis artículos, pero de 155 considerandos y siete anexos donde se recogen los compromisos adquiridos por los organismos estadounidenses.

45. El *Privacy Shield* es un mecanismo de autocertificación de empresas sitas en EE.UU en el que se permite la transferencia de datos a las empresas que hayan sido certificadas mediante el cumplimiento de unos requisitos de seguridad y el cumplimiento de unos principios avalados por el Departamento Federal de Comercio. Las empresas certificadas se incluirán en una lista publicada por las autoridades estadounidenses en las que se muestran todas las empresas que han superado el proceso de autocertificación. Esas empresas deberán renovar anualmente su autocertificación. Del mismo modo, deberán tomar medidas para verificar que las políticas de privacidad que han publicado se ajustan a los principios y se aplican.

---

[47] Contenido de los artículos reformados por la Decisión de ejecución 2016/2295:

Artículo 3:

Cuando las autoridades competentes de los Estados miembros ejerzan sus facultades con arreglo al artículo 28, apartado 3, de la Directiva 95/46/CE, y ello dé lugar a la suspensión o la prohibición definitiva de los flujos de datos hacia [del Estado] con el fin de proteger a las personas en lo que respecta al tratamiento de sus datos personales, el Estado miembro afectado informará inmediatamente a la Comisión, que remitirá la información a los demás Estados miembros.

Artículo 3 bis o artículo 4:

1. La Comisión realizará un seguimiento continuo de toda evolución del ordenamiento jurídico [del Estado] que pueda afectar al funcionamiento de la presente Decisión, y en particular de la evolución de las normas que regulan el acceso a los datos personales por parte de las autoridades públicas, con el fin de determinar si [del Estado] sigue garantizando un nivel adecuado de protección de los datos personales.

2. Los Estados miembros y la Comisión se informarán recíprocamente de aquellos casos en que la actuación de los organismos responsables del cumplimiento de las normas de protección en [del Estado] no garantice dicho cumplimiento.

3. Los Estados miembros y la Comisión se informarán recíprocamente cuando haya algún indicio de que las injerencias por parte de los poderes públicos [del Estado] competentes en materia de seguridad nacional, aplicación de la ley u otros intereses públicos en el derecho de las personas a la protección de sus datos de carácter personal van más allá de lo estrictamente necesario, o de que no existe una tutela judicial efectiva frente a tales injerencias.

4. Si se demuestra que ya no está garantizado un nivel adecuado de protección, incluso en las situaciones a que se refieren los apartados 2 y 3 del presente artículo, la Comisión informará de ello a la autoridad competente [del Estado] y, en caso necesario, propondrá un proyecto de medidas de conformidad con el procedimiento a que se refiere el artículo 31, apartado 2, de la Directiva 95/46/CE, a fin de anular o suspender la presente Decisión, o limitar su ámbito de aplicación.

[48] DO L 207/1, de 1 de agosto de 2016.

46. Como diferencias principales respecto al *Safe Harbour*, encontramos[49]:

1) El nombramiento del *ombudsman* dentro del Departamento de Estado al que las autoridades de protección de datos pueden presentar peticiones en nombre de ciudadanos europeos sobre las prácticas de inteligencia de señales de Estados Unidos. El *ombudsman* solo recibirá peticiones de ciudadanos europeos y no de ciudadanos de Cualquier otra región o de los ciudadanos estadounidenses.
2) Al igual que con *Safe Harbour*, las compañías que voluntariamente acuerdan unirse a *Privacy Shield* deben obtener el consentimiento de los europeos antes de compartir datos con terceros, incluido el consentimiento expreso para compartir datos sensibles, como información de salud, y permitir a los europeos acceder, corregir o borrar sus datos transferidos. Además, las empresas miembros de *Privacy Shield* tendrán que asegurar a través de contratos que sus socios de negocios que reciben información sobre los europeos también pueden cumplir con todos estos principios. Y las compañías adheridas al *Privacy Shield* tendrán nuevas y continuas obligaciones de supervisar las actividades de procesamiento de sus agentes.
3) El *Privacy Shield* también refuerza la aplicación y el recurso del consumidor. La Comisión interpuso casi cuarenta casos en los últimos cinco años contra compañías que violaron los principios de *Safe Harbour* o falsificaron su participación en el programa. Bajo el *Privacy Shield*, algunas de estas violaciones pueden ser detectadas y detenidas antes de que se haga necesaria una acción coercitiva porque el Departamento de Comercio de EE.UU. deberá vigilar de cerca los registros y la participación de *Privacy Shield*. Al mismo tiempo, Los ciudadanos europeos gozan de un sistema escalonado de recursos y reclamaciones que estudiaremos a continuación.

2. Principios del *Privacy Shield*

47. El *Privacy Shield* se aplica tanto a los responsables como a los encargados del tratamiento, si bien estos deben estar obligados, por contrato, a actuar únicamente siguiendo instrucciones del responsable del tratamiento de la Unión Europea y asistir a este último a responder a las personas físicas que ejerzan sus derechos con arreglo a los siguientes principios que, *a priori,* parecen superar en garantías al *Safe Harbor*[50]:

1. Derecho a ser informado: Las empresas estadounidenses estarán obligadas a informar a los titulares de los datos sobre los aspectos clave en el procesamiento de sus datos de carácter personal (tipos de datos recopilados, propósito del tratamiento de los datos, derechos de acceso a la información y condiciones de transmisión o cesión de dichos datos a un tercero, medios de contacto con la empresa, órgano de resolución de controversias, autoridad de control de EE.UU). Además de diversas obligaciones formales (i) su adhesión al *Privacy Shield* y la indicación del enlace a la lista de entidades adheridas al mismo; (ii) los tipos de datos que se han recogido; (iii) el compromiso que tiene la entidad de cumplir con dichos principios; (iv) la finalidad para la cual se recogen los datos; (v) el procedimiento para contactar con la entidad para presentar reclamaciones y quejas).
2. Derecho de elección: Las empresas estadounidenses deberán obtener el consentimiento formal por parte de los ciudadanos antes de ceder sus datos personales sensibles a entidades terceras o se utiliza para un fin distinto por el que se recabaron los datos en un principio.
3. Principio de seguridad: Las empresas estadounidenses deberán evaluar los riesgos de seguridad en el tratamiento de la información de carácter personal y deberán implantar medidas

[49] *Vid*. J. Brill, "Strengthening International Ties Can Support Increased Convergence of Privacy Regimes", *European Data Protection Law Review*, vol. 2, nº 2, Berlin, Lexxion, 2016, pp. 1514-155.

[50] *Vid*. R. Pérez Cambero, "Aspectos más destacables de la Decisión de Ejecución 2016/1250 de la Comisión Europea, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU", *Actualidad Administrativa*, nº. 4, 2017, p. 3.

de seguridad que mitiguen al máximo riesgos como pérdidas, mal uso, acceso no autorizado, revelación, alteración o destrucción de estos datos. En el caso de que la entidad subcontrate a un tercero de un servicio determinado, se le deberá exigir un nivel de seguridad equivalente al requerido por la entidad para la protección de la información de carácter personal tratada.

4. Principio de integridad y limitación de la finalidad: Las empresas estadounidenses deberán garantizar la integridad de los datos personales obtenidos; el titular de los datos sólo deberá ser revelado en los casos en que esto sea imprescindible. La limitación de la finalidad de los datos implica que los datos de carácter personal recabados deben ser relevantes para los fines del tratamiento. Únicamente se permite guardar los datos personales en tanto resulten necesarios para el propósito del tratamiento. A dichas empresas se les permitirá conservar datos durante periodos más prolongados exclusivamente en caso de que los necesite para determinados fines en particular, tales como archivo por interés público, periodismo, literatura y arte, investigación científica o histórica, o para análisis estadístico (los mismos que se recogen en el RGPD). Si el nuevo fin es sustancialmente distinto, la empresa sujeta al Escudo de Privacidad solo podrá usar sus datos si no se pone ninguna objeción o, en caso de tratarse de datos sensibles, si da su consentimiento. Si el nuevo fin esta bastante relacionado con el original, su uso es permisible. Existe el derecho a elegir si los datos enviados a una empresa sujeta al escudo pueden transferirse a otra empresa, sea de EEUU o no.
5. Derecho de acceso y rectificación de sus datos: Las empresas estadounidenses deberán informar a los titulares de los datos sobre el contenido de los datos que obran en su poder y deberá facilitarles el acceso a dichos datos en un plazo de tiempo razonable, salvo que suponga un esfuerzo desproporcionado. Se podrá solicitar a la empresa que los corrija, los cambie o los elimine si no son exactos, están desfasados o han sido procesados infringiendo las normas del Escudo de Privacidad. La empresa deberá también confirmar si guarda y procesa o no sus datos personales. Las peticiones de acceso a su información personal podrán ser efectuadas por los ciudadanos en cualquier momento. Por lo general, no se obliga a dar ninguna razón acerca de los motivos por los que desea acceder a sus datos; no obstante; la empresa podrá pedirle que lo haga si su solicitud es demasiado genérica o vaga.
6. Principio de responsabilidad para transmisiones lícitas: Como elemento común, se pueden transmitir datos a terceros de manera lícita solo si existe justificación expresa. Si se va a transferir los datos a un tercero responsable de los datos, deberán cumplir los principios de notificación y opción. Las entidades deberán requerir, a través de un acuerdo por escrito, que las terceras partes que reciban los datos personales otorguen el mismo nivel de protección que el que proporciona el *Privacy Shield*. Si se realiza a un tercero que actúe como encargado del tratamiento, la entidad deberá de asegurarse, entre otras, de que este tratará los datos únicamente para los fines para los que fueron recabados.
7. Derecho a reclamar y ser indemnizado: Las empresas estadounidenses deberán implantar sistemas de verificación del cumplimiento de los principios del *Privacy Shield* y deberán informar de su cumplimiento de manera anual por medio de la renovación de su autocertificación, donde deberán acreditar las acciones que han adoptado para ceñirse a los principios del *Privacy Shield*. En el caso de que las empresas afectadas no demuestren el cumplimiento de dichos requerimientos, saldrán de la lista de empresas adheridas al *Privacy Shield* y estarán sujetas a sanciones económicas.

48. Si se considera que se han vulnerado los derechos y ha recibido un perjuicio, se tiene derecho a reclamar mediante las siguientes y numerosas instancias de forma sucesiva:

i Ante la propia empresa estadounidense sujeta al Escudo de Privacidad.
ii Mediante un mecanismo de recurso independiente.
iii Ante el Departamento de Comercio de los EE. UU.
iv Ante la Comisión Federal de Comercio de los EE. UU.
v. Ante el Panel del Escudo de Privacidad en EE.UU, solo después de que hayan fracasado las

demás opciones.

3. Críticas y amenazas al *Privacy Shield*

49. Pero no todo es positivo en esta nueva decisión: la poca rigidez en las obligaciones impuestas a los Estados Unidos[51], el lenguaje ambiguo, poco claro, y difícil de entender en algunos aspectos debido a la discrepancia en la interpretación de los conceptos por parte de la UE y EE.UU.[52], y las nuevas reformas emprendidas por el axtual gobierno de Estados Unidos han supuesto una pérdida de protección de la privacidad, como la *Executive Order on Public Safety*[53], que excluye la aplicación de la ley de protección de datos estadounidense a las personas extranjeras en Estados Unidos, o la derogación de la *rule submitted by the Federal Communications Commission relating to "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services"* (FISA)[54] y se ha promulgado la renovación de la Sección 702 *U.S. Foreign Intelligence Surveillance Act*, que permite a las agencias de inteligencia acceder a datos de personas no estadounidenses y la *Clarifying Lawful Overseas Use of Data Act* que permite el acceso a datos personales establecidos en servidores de otros países de empresas estadounidenses.

50. Podemos calificar al escudo de privacidad de "suave actualización", sobre todo en los pocos avances en la mejora de los principios de notificación y elección, puesto que solo cubren el cambio de fin para realizar el tratamiento; todas las operaciones típicas de procesamiento (por ejemplo, recopilación, almacenamiento, creación de perfiles, vinculación de datos) ni siquiera están cubiertas por los principios de notificación y elección[55]. Tanto el Parlamento Europeo[56] y el CEPD en su WP255 han criticado profundamente la falta de medias adoptadas la Administración estadounidense, llegando a solicitar la suspensión de la Decisión; a diferencia de lo considerado por la Comisión Europea, que tras sus dos revisiones anuales consideran continúa asegurando un nivel adecuado a los datos personales transferidos bajo el *Privacy Shield* a las organizaciones adheridas[57]. Aún así, la Comisión recomienda algunas medidas destinadas a asentar el propio mecanismo en un tono muy laxo.

51. Los elementos que hacen dudar de la legalidad de la Decisión respecto a la CDFUE son:

a) La recopilación de datos indiscriminada a las agencias de inteligencia y seguridad en virtud de FISA y la Orden Ejecutiva 12333.
b) La supervisión de los programas de vigilancia, llevada a cabo por la Privacy and Civil Liberties Oversight Board, la cual actualmente no se encuentra totalmente en funcionamiento por la falta de miembros derivada de la transición del gobierno.
c) Las dificultades de un ciudadano europeo de solicitar una indemnización en procesos penales en casos de *surveillance.*
d) La ausencia de ombudsperson como órgano independiente que se prometió por parte del gobierno estadounidense para dilucidar las reclamaciones efectuadas para otorgar un mejor resultado que los tribunales.

52. Todas estas inseguridades han culminado en una petición de decisión prejudicial por parte la *High Court* irlandesa derivado de un conflicto que vuelve a involucrar a Facebook y Max Schrems, instando al TJUE[58] a pronunciarse sobre:

---

[51] *Vid*. Sección tribuna, "El 'Escudo de Privacidad` entre la UE y EE.UU. necesita mejorar", *Diario La Ley*, Nº 8760, 2016.

[52] *Vid*. S. Bu-Pasha, "Cross-border issues under EU data protection law with regards to personal data protection", *Information & Communications Technology Law*, Routledge, 2017, p. 12.

[53] Executive Order 13768. 27 de enero de 2017.

[54] Public Law 115-22 (04/03/2017).

[55] *Vid*. M. Schrems, "The Privacy Shield is a Soft Update of the Safe Harbor", *European Data Protection Law Review*, vol. 2, N.º 2, 2016, pp. 148-150.

[56] (2016/3018(RSP)).

[57] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield (COM (2017) 611 final).

[58] Petición de decisión prejudicial planteada por la *High Court* (Irlanda) el 9 de mayo de 2018 — Data Protec-

a) Los criterios para valorar si la legislación y las prácticas de una transferencia de datos a un tercer Estado que puede tratar dichos datos personales para fines de seguridad nacional pueden vulnerar los derechos de las personas.
b) Las garantías ofrecidas por la legislación estadounidense.
c) Las garantías contractuales mínimas que deberían ofrecer las Cláusulas Contractuales tipo.
d) La idoneidad del *Privacy Shield* como medio para constatar que las garantías ofrecidas por EE. UU son adecuadas, y su vinculación con las transferencias de datos personales a EE. UU conforme a las Cláusulas Contractuales Tipo aprobadas por la Comisión Europea.
e) La idoneidad del *ombudsperson* como garantía adecuada.
f) La vulneración de las Decisiones sobre Cláusulas Contractuales Tipo aprobadas por la Comisión Europea (Decisiones 2010/87/UE y 2001/497/CE) a la luz de la CDFUE.

53. Las cuestiones planteadas ponen en tela de juicio los instrumentos más relevantes que posee la Unión Europea para permitir el movimiento internacional de los datos personales, al primar por parte de la Comisión Europea los intereses comerciales que el propio derecho a la protección de datos de los ciudadanos europeos. La Comisión ha sido, y es cuestionada por sus decisiones en esta materia, lo que ponen en una situación de desconfianza hacia esta institución. El mecanismo actual para aprobar una decisión de adecuación tiene su punto débil en el carácter no vinculante del dictamen emitido por el CEPD, cuya oportunidad se ha perdido al no otorgar un carácter vinculante al dictamen emitido por este órgano.

4. Los mecanismos judiciales de control de la legalidad de las decisiones sobre transferencias internacionales de datos ante la Comisión Europea en la legislación de los Estados miembros

54. Vistos los antecedentes en esta materia y los problemas que nos encontramos actualmente con las decisiones de la Comisión Europea, el RGPD ha previsto en el artículo 58.5 un mecanismo obligatorio para los Estados miembros de articular mecanismos a favor de las autoridades de control que permitan fiscalizar las infracciones en materia de protección de datos y permitir a las autoridades de control poner en conocimiento de los tribunales dichas infracciones y, si procede, instar acciones judiciales para hacer cumplir el RGPD. La sentencia de 6 de octubre de 2015, asunto C-362/14, Schrems, en su párrafo 65[59] impuso por primera vez esta obligación en los Estados miembros, y traducido a esta materia, impone a los Estados miembros

55. En los diferentes Estados miembros, se han adoptado medidas idénticas o similares con el fin de hacer cumplir el mandato legal del RGPD, y con la protección de los derechos fundamentales. La solución admitida por los Estados miembros se basa, principalmente, en mecanismos de autorización judicial solicitados a instancia de la autoridad de control para solicitar la suspensión de la transferencia internacional basa en las decisiones de la Comisión Europea y presentar ante el TJUE una cuestión prejudicial para determinar la validez del acto.

56. Alemania fue el primer Estado en adaptar su legislación al RGPD, e ideó el mecanismo de autorización judicial que han copiado el resto de Estados. Regula un procedimiento más completo en la Sección 21 de la *Bundesdatenschutzgesetz* de junio de 2017[60], al establecer un procedimiento judicial

tion Commissioner / Facebook Ireland Limited, Maximillian Schrems (Asunto C-311/18).

[59] "En el supuesto contrario, cuando esa autoridad considere fundadas las alegaciones expuestas por la persona que le haya presentado una solicitud para la protección de sus derechos y libertades frente al tratamiento de sus datos personales, la referida autoridad debe tener capacidad para comparecer en juicio, conforme al artículo 28, apartado 3, párrafo primero, tercer guion, de la Directiva 95/46, entendido a la luz del artículo 8, apartado 3, de la Carta. A ese efecto, corresponde al legislador nacional prever las vías de acción que permitan a la autoridad nacional de control exponer las alegaciones que juzgue fundadas ante los tribunales nacionales, para que éstos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de la Comisión, planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de ésta."

[60] §21 Bundesdatenschutzgesetz: *(1) If a supervisory authority believes that an adequacy decision of the European Commission or a decision on the recognition of standard protection clauses or on the general validity of approved codes of conduct, on the validity of which a decision of the supervisory authority depends, violates the*

basado en un procedimiento específico contenido en la propia Ley, y en las leyes procesales para ventilar la solicitud emanada de las autoridades de control. A su vez, contempla un trámite de audiencia a la Comisión Europea para presentar alegaciones en un plazo determinado por el Tribunal Administrativo Federal. Este sistema es muy similar al planteado en Holanda, con la salvedad de no recoger un periodo de alegaciones por parte de la Comisión Europea.

57. En Francia resaltamos el artículo 43 de la *Loi* n° 78-17 de 6 de enero de 1978, reformada por la *Loi* n° 2018-493 de 20 de junio de 2018[61] que, de manera idéntica, pero con una mejor redacción, aplica el mismo mecanismo de autorización, que en su caso recae sobre el Consejo de Estado francés, con la diferencia de aplicar únicamente a las decisiones de adecuación de un tercer Estado u Organización Internacional, y aplicarse el mismo procedimiento a las decisiones de adecuación del artículo 36 de la Directiva 680/2016.

58. En el caso de España, en la disposición adicional quinta de la LO 3/2018 PDyGDD[62], redactado de manera confusa, consiste en la suspensión de un procedimiento concreto por parte de la autori-

---

law, the supervisory authority shall suspend its procedure and lodge an application for a court decision.

(2) Recourse to the administrative courts shall be provided for proceedings pursuant to subsection 1. The Code of Administrative Court Procedure shall be applied in compliance with subsections 3 to 6.

(3) The Federal Administrative Court shall decide in the first and last instance on an application by the supervisory authority pursuant to subsection 1.

(4) In proceedings pursuant to subsection 1, the supervisory authority shall be competent to take part. The supervisory authority shall be a party to proceedings pursuant to subsection 1 as applicant; Section 63 nos. 3 and 4 of the Code of Administrative Court Procedure shall remain unaffected. The Federal Administrative Court may give the European Commission the opportunity to comment within a period of time to be determined.

(5) If a proceeding to review the validity of a European Commission decision pursuant to subsection 1 is pending at the European Court of Justice, the Federal Administrative Court may order its proceeding to be suspended until the proceeding at the European Court of Justice has been concluded.

(6) In proceedings pursuant to subsection 1, Section 47 (5), first sentence and (6) of the Code of Administrative Court Procedure shall apply accordingly. If the Federal Administrative Court finds that the European Commission's decision pursuant to subsection 1 is valid, it shall state this in its decision. Otherwise it shall refer the question as to the validity of the decision in accordance with Article 267 of the Treaty on the Functioning of the European Union to the European Court of Justice.

61 Art. 47 Loi n° 78-17: *Dans le cas où, saisie d'une réclamation dirigée contre un responsable de traitement ou son sous-traitant, la Commission nationale de l'informatique et des libertés estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne à l'égard du traitement de ses données à caractère personnel, ou de manière générale afin d'assurer la protection de ces droits et libertés dans le cadre de sa mission, elle peut demander au Conseil d'Etat d'ordonner la suspension d'un transfert de données, le cas* échéant *sous astreinte, et elle assortit alors ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne en vue d'apprécier la validité de la décision d'adéquation de la Commission européenne prise sur le fondement de l'article 45 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ainsi que de tous les actes pris par la Commission européenne relativement aux garanties appropriées dans le cadre des transferts de données mentionnées à l'article 46 du même règlement.*

62 DA 5ª: 1. *Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.*

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquéllas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquéllas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquéllas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

dad de control cuya resolución depende de la validez de una decisión emanada de la Comisión Europea concerniente a la a) adecuación de un tercer Estado u Organización Internacional, b) la aprobación de cláusulas contractuales tipo, y c) la validez de códigos de conducta a tal efecto que pueden suponer una vulneración del derecho a la protección de datos, para que la autoridad de control solicite una autorización al órgano judicial competente con el fin de poder declarar dicha transferencia de datos personales contraria a Derecho. En su admisión a trámite, el órgano judicial confirmará o no la suspensión y, en caso afirmativo, elevará ante el TJUE una petición de cuestión prejudicial sobre la validez de la decisión emanada de la Comisión Europea. Si el TJUE declarase contraria a Derecho la decisión de la Comisión Europea, el órgano judicial nacional competente concederá la autorización a la autoridad de control y prohibirá la transferencia internacional de datos personales.

59. Los órganos judiciales competentes a los que puede dirigirse a la autoridad de control varía según su condición: si la solicitud la realizase de Consejo General del Poder Judicial, el órgano será la Sala Tercera del Tribunal Supremo; si lo realizase la AEPD, será la Sala Tercera de la Audiencia Nacional, y si lo solicitase una autoridad autonómica, será la Sala Tercera del Tribunal Superior de Justicia.

60. El procedimiento para obtener dicha autorización se encuentra en el artículo 122 ter de la Ley 29/1998, reguladora de la Jurisdicción Contencioso-administrativa. El procedimiento comenzará con la petición de la autoridad de protección de datos ante el órgano competente. Los intervinientes en el procedimiento serán la autoridad de protección de datos, quienes lo fueran en el procedimiento anterior, y la Comisión Europea. Podrá celebrarse una vista si el tribunal lo ve necesario tras la petición de alguna de las partes. La resolución que dicte el tribunal estará sujeta a los recursos pertinentes.

61. En Irlanda, lugar que podemos aceptar como el germen de estas nuevas previsiones, regula un mecanismo más programático que práctico en la *Data Protection Act 2018* con el mismo fondo que los anteriores, alcanzando a las decisiones de adecuación y de aprobación de cláusulas contractuales tipo.

62. El mecanismo de autorización judicial ha primado sobre el sistema de recurso directo por parte de la autoridad de control, al configurar esta como un "órgano jurisdiccional" a efectos del Derecho de la Unión[63] que permita a las autoridades de control tener un cauce directo con el TJUE sin necesidad de procedimentalizar en demasía el mecanismo, como observamos en los distintos ordenamientos de los Estados miembros. Según las disposiciones de la jurisprudencia del TJUE, un órgano administrativo puede considerarse como tal si se cumplen los requisitos de legalidad, carácter permanente, competencia obligatoria, procedimiento contradictorio, aplicación de normas legales, e independencia del órgano[64]; criterios que las autoridades de control cumplen al:

a) Ser creado no para situaciones concretas en el tiempo (permanencia),
b) Tener los interesados la obligación de acudir ante las autoridades de control para dirimir cualquier reclamación (competencia obligatoria),
c) Contemplar procedimientos contradictorios como la presentación de pruebas y alegaciones (Procedimientos contradictorios),
d) Al aplicar normas legales como el RGPD y demás legislación sobre protección de datos (Aplicar normas de derecho),
e) Configurarse como órganos independientes por tanto por los considerandos 116, 117, 121 y la sección 1ª del Capítulo VI del RGPD (independencia).

63. Este sistema fue planteado por el Consejo General del Poder Judicial en su informe complementario del 26 de octubre sobre el Anteproyecto de Ley Orgánica de Protección de Datos pero que, finalmente, no fue aceptado.

[63] Ya se admitió una petición de decisión prejudicial por el Tribunal Catalán de Contratos de Sector público en la STJUE de 6 de octubre de 2015, *Consorci Sanitari del Maresme*, C-203/14.

[64] SSTJUE 30 de junio de 1966, *Vaassen- Göbbels,* C-61/65, y 11 de junio de 1987, *Pretore di Salò*, C-14/86.

64. En definitiva, el mecanismo de autorización pretende revestir de carácter jurisdiccional y mayor autoridad a la cuestión planteada, además de dotar de mayor formalismo y garantía a un procedimiento tan sensible como la búsqueda de invalidez de una decisión de la Comisión Europea con tanta repercusión en el Mercado Único Digital.

VI. La Decisión de ejecución de 23 de enero de 2019 sobre la adecuación de la protección de los datos personales que ofrece Japón

65. El 23 de enero de 2019 entró en vigor la Decisión de ejecución que permite la transferencia internacional de datos personales a Japón. Esta decisión es la primera emitida sobre la base del nuevo régimen vigente sobre protección de datos, y la estructura cambia sustancialmente con las anteriores decisiones.

66. La Decisión consta de 191 Considerandos donde se analiza la legislación japonesa sobre protección de datos y la idoneidad para promulgar la adecuación, y 4 artículos donde regula obligaciones aplicables a la Comisión y a los Estados miembros. Adicionalmente, se han aportado unas reglas supletorias otorgadas por Japón que permiten encajar algunos términos discordantes o incompatibles con la legislación europea.

67. Los Considerandos se estructuran según el análisis de los conceptos claves de la legislación japonesa:

a) La legislación japonesa aplicable.
b) El concepto de dato personal. Japón diferencia los conceptos de "dato personal" de "información personal", siendo el criterio diferenciador la estructura de los datos, considerando los datos estructurados que te permitan identificar directamente a una persona como "datos personales".
c) El concepto de anonimización que, atendiendo a la concepción japonesa, se asemeja con el de seudonimización al no cubrir los supuestos de reidentificación. para cubrir esta carencia, se otorga un nuevo concepto para los datos transferidos por la Unión Europea en las normas supletorias, contemplando estos supuestos.
d) Los conceptos de responsable y encargado. En Japón no se concibe esta distinción de supuestos, por lo que cualquier movimiento entre entidades serán considerados responsables ante la norma. Esta previsión, se considera, no afecta al nivel de protección prestado.
e) Exclusiones sectoriales. La legislación japonesa excluye una serie de tratamientos en los que no son de aplicación las salvaguardas de la legislación japonesa[65]. Para cubrir dichos supuestos, estos tratamientos estarán cubiertos por legislación japonesa si, tras la transferencia internacional de datos personales inicial con una finalidad no excluida de la aplicación, hubiese un tratamiento ulterior para una finalidad excluida, dicho tratamiento ulterior estará protegida por la Decisión y la legislación japonesa en su totalidad.
f) La consonancia con los principios de tratamiento japoneses con los europeos, los cuales encuentran similitud de contenido con los mencionados en el RGPD.
g) Los derechos de los afectados, los cuales contienen un catálogo similar al europeo destacan-

[65] (i) instituciones de radiodifusión, editores de periódicos, agencias de comunicación u otras organizaciones de prensa (incluidas las personas que realicen actividades de prensa como su negocio) en la medida en que procesen información personal para fines de prensa; (ii) personas dedicadas a la escritura profesional, en la medida en que esto involucre información personal; (iii) universidades y cualquier otra organización o grupo dirigido a estudios académicos, o cualquier persona que pertenezca a dicha organización, en la medida en que procesen información personal para fines de estudios académicos; (iv) organismos religiosos en la medida en que procesen información personal para fines de actividad religiosa (incluidas todas las actividades relacionadas); y (v) cuerpos políticos en la medida en que procesen información personal para los fines de su actividad política.

do los tradicionales ARCO.

h) La existencia de una autoridad de supervisión independiente y la capacidad de aplicar la ley y sancionar a los infractores.
i) La existencia de recursos judiciales, los cuales se contemplan en diferentes jurisdicciones, además de permitir al usuario reclamar ante el propio responsable.
j) Las limitaciones a los derechos de los usuarios en los casos de accesos por administraciones públicas japonesas.

68. El resto del articulado se centra en la declaración de la legislación japonesa de protección de datos como adecuada para permitir la transferencia de datos personales desde la Unión Europea hacia Japón. Dentro del propio articulado se impone la comunicación a la Comisión Europea de cualquier suspensión o prohibición realizada por la autoridad de control para impedir la transferencia de datos a las entidades sujetas a la legislación japonesa de protección de datos.

69. Podemos afirmar las medidas aportadas por Japón suponen un nivel adecuado de protección suficiente para permitir la transferencia internacional de datos a este tercer Estado. En especial, la adopción de las reglas supletorias proporcionadas por Japón suponen un esfuerzo legislativo para dar una interpretación que permita adecuar la legislación.

VII. Conclusiones

70. Las Decisiones de adecuación suponen el principal instrumento legislativo de la Unión Europea para permitir una mayor libertad de flujo transfronterizo de datos. En las normas europeas y en todos los instrumentos de *soft law* de la Comisión y Comité Europeo de Protección de Datos se puede observar la gran influencia de la STJUE *Schrems* en la redacción del artículo 45 del RGPD, sobre todo en la obligación de supervisión continua por parte de la Comisión en los propios sujetos a una Decisión de adecuación con el objetivo de no repetir este episodio. El triple mecanismo de control del cual son objeto las Decisiones de adecuación se presenta en principio como una herramienta útil que pretende eliminar los vicios pasados de las anteriores Decisiones, y que en las sucesivas que se promulguen se observará la eficacia de la medida.

71. La Decisión 2016/1250 de la Comisión, por el que se aprueba el mecanismo de *Privacy Shield* se encuentra actualmente en el punto de mira debido a las nuevas políticas del actual gobierno de EE. UU, y esta Decisión se convertirá en un verdadero examen para la Comisión en aplicación del artículo 45 del RGPD. El *Privacy Shield* muestra importantes puntos débiles muy complicados de casar con la jurisprudencia europea y el actual RGPD, y los miedos se han traducido en una cuestión prejudicial para confirmar la validez de las decisiones relativas a la adecuación del *Privacy Shield* y las cláusulas contractuales tipo. Esta cuestión prejudicial puede sumir el régimen de las transferencias internacionales de datos en una crisis sin precedentes al estar en vilo las bases del propio sistema.

72. En cambio, la Decisión de adecuación de Japón supone todo un ejemplo de diligencia por parte de la Comisión Europea a la hora de permitir una transferencia internacional de datos, permitiendo la implicación de otros órganos no preceptivos que opinen sobre la adecuación del Estado u organización internacional, con la consecuencia de reforzar las valoraciones de la Comisión.

73. Tanto el RGPD como la Directiva 2016/680 han otorgado a los Estados miembros, mediante la adaptación al Derecho nacional, más herramientas para controlar la legalidad de los actos de adecuación de la Comisión Europea, la cual se ha visto superada por las vicisitudes políticas, mediante el planteamiento de una cuestión prejudicial en el caso de que una autoridad de control considere que una decisión de la Comisión Europea puede vulnerar los derechos y libertades, otorgando más flexibilidad e inmediatez al control efectuado por el Estado miembro.