¿Y a la tercera va la vencida?... El nuevo marco transatlántico de privacidad de datos UE-EE.UU.

And the third time is a win?... The new EU-US transatlantic data privacy framework

Alfonso Ortega Giménez
Profesor Titular de Derecho internacional privado
Universidad Miguel Hernández de Elche
ORCID: 0000-0002-8313-2070

Recibido:08.11.2023 / Aceptado:30.11.202
DOI: 10.20318/cdt.2024.8432

Resumen: IEl nuevo Marco de Privacidad de Datos UE-EE.UU. introduce nuevas garantías vinculantes al objeto de dar respuesta a cada uno de los motivos de inquietud puestos de manifiesto por el TJUE, en su día, en las Sentencias «Schrems I» y «Schrems II». Entre estas garantías se encuentran la limitación del acceso por parte de los servicios de inteligencia estadounidenses a los datos de la UE y el establecimiento de un Tribunal de Recurso en Materia de Protección de Datos, al que los ciudadanos de la UE tendrán acceso. Esperemos que con la aprobación de este nuevo Marco de Privacidad de Datos se pueda no sólo «cerrar», definitivamente, la falta de garantías señalada por el TJUE y que provocó la invalidez de los dos marcos de privacidad anteriores (Safe Harbor y Privacy Shield) sino, sobre todo, establecer un nuevo marco seguro y duradero, mediante el que se puedan realizar las transferencias de datos personales necesarias UE-EE.UU. Este trabajo se centra en el estudio de los diferentes esfuerzos llevados a cabo a nivel jurídico para establecer un marco regulatorio satisfactorio para las transferencias internacionales de datos de carácter personal UE-EE.UU., haciendo especial hincapié en el nuevo Marco transatlántico de Privacidad de Datos, recientemente aprobado.

Palabras clave: Transferencias internacionales, protección de datos, privacidad, marco transatlántico.

Abstract: The new EU-US Data Privacy Framework introduces new binding safeguards to address each of the concerns raised by the CJEU in the 'Schrems I' and 'Schrems II' judgments. Among these guarantees are the limitation of access by US intelligence services to EU data and the establishment of a Data Protection Court of Appeal, to which EU citizens will have access. Hopefully, with the approval of this new Data Privacy Framework, it will be possible not only to "close", definitively, the lack of guarantees pointed out by the CJEU and which led to the invalidity of the two previous privacy frameworks (Safe Harbor and Privacy Shield) but, above all, to establish a new secure and durable framework, through which the necessary EU-US transfers of personal data can be carried out, with special emphasis on the recently adopted new Transatlantic Data Privacy Framework.

Keywords: International transfers, data protection, privacy, transatlantic framework.

I. Antecedentes en la regulación de las transferencias internacionales de datos de carácter personal desde la UE a entidades ubicadas en los EE.UU

1. La Directiva 95/46/CE supuso el inicio de una disputa entre la UE y los EE.UU., ya que, a los ojos de la Directiva, era posible que las exportaciones de datos de carácter personal a los EE.UU. fueran prohibidas ya que mientras el enfoque de EEUU en esta materia se basaba en una mezcla de legislación, reglamentación y autorregulación, la UE consideraba imprescindible la protección del derecho fundamental a la privacidad.

2. Tras largas negociaciones, el 29 de julio de 2000, la UE y los EE.UU. llegaron a un acuerdo, denominado *Safe Harbour Principles* (Principios de Puerto Seguro) por el que se establecía un sistema para la protección de la vida privada, una auténtica suerte de extensión de la regulación vigente en la UE en materia de protección de datos de carácter personal. Se trataba de un sistema eficaz, tanto desde el punto de vista teórico como desde el punto de vista práctico, ya que posibilita un flujo estable e ininterrumpido de información asegurando un nivel permanente de protección adecuada.

3. El sistema de Principios de Puerto Seguro, aunque fue criticado en algunas ocasiones, presentaba numerosas ventajas, teniendo en cuenta que: a) constituyó un marco normativo uniforme, permanente, estable y definitivo para la protección del derecho a la intimidad y para la transferencia internacional de datos de carácter personal entre la UE y los EE.UU.; b) permitió la aprobación automática por todos los Estados miembros de la UE de las transferencias internacionales de datos de carácter personal con destino a los EE.UU.; y, c) sustituyó a las legislaciones internas de cada uno de los Estados miembros de la UE.

4. La razón de ser de los Principios de Puerto Seguro fue el hecho de que EE.UU. se rige, en numerosos ámbitos, por el principio de autorregulación, en virtud del cual son las propias empresas las que adoptan sus propios códigos de conducta o se acogen a códigos de conducta sectoriales, respecto de los cuales el Estado carece de facultad fiscalizadora o de control alguno. Para suplir esta laguna se crean los principios de *Safe Harbour*, un sistema que trata de conjugar la autorregulación estadounidense con el régimen jurídico comunitario en esta materia.

5. La empresa que se quería adherir a este Sistema debía presentar una carta de autocertificación ante el Departamento de Comercio, por la que manifiestaba su adhesión a los principios y *FAQ*, así como indicando, en particular, los datos de identificación de la entidad solicitante, una descripción de su actividad en lo relativo a la información personal recibida de la UE y una descripción de su política de protección de datos de carácter personal.

6. El sistema de Principios de Puerto Seguro se configuró, entonces, como un programa voluntario, basado en la autocertificación y en la autoevaluación, que se ofrece a las entidades de los EE.UU. con el fin de obtener, respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida en el ámbito comunitario, que permite asegurar, de manera permanente, la legitimidad de las transferencias internacionales de datos de carácter personal.

7. Los Principios de Puerto Seguro, que se configuraron como mínimos para cualquier política privada de protección de datos de carácter personal, fueron los siguientes:

1º) **Principio de "Notificación" (*Notice*):** establece la obligación que tienen las entidades de informar a los particulares de los fines y utilización de sus datos de carácter personal.
2º) **Principio de "Opción" (*Choice*):** dispone la obligación de las entidades de ofrecer a los particulares la posibilidad de decidir si sus datos de carácter personal pueden ser o no cedidos a un tercero.
3º) **Principio de "Transferencia Ulterior" (*Onward Transfer*):** señala que para revelar información a terceros que no participen en el sistema de Puerto Seguro, las entidades deberán aplicar los Principios de notificación y de opción.
4º) **Principio de "Seguridad" (*Security*):** establece que las entidades que se encargan de la recogida de datos de carácter personal deberán tomar todas las precauciones que estimen oportunas con el fin de evitar su pérdida, modificación o destrucción.
5º) **Principio de "Integridad de los datos" (*Data Integrity*):** señala que los datos de carácter personal deben ser pertinentes con respecto a los fines con los que se utiliza.
6º) **Principio de "Acceso" (*Access*):** recoge el derecho de los particulares al conocimiento de sus datos de carácter personal que las entidades tengan sobre ellos y poder corregirla, modificarla o suprimirla en caso de que sea inexacta.
7º) **Principio de "Aplicación" (*Enforcement*):** dispone la necesidad de incluir una vía de recurso para los interesados que se vean afectados por el incumplimiento de la normativa sobre transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

8. Aunque existían toda una serie de excepciones a estos Principios del sistema de Puerto Seguro, cuando era necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley, cuando una disposición legal o resolución jurisdiccional así lo estableciera y/o cuando la Directiva 95/46/CE o cualquier norma de los Estados miembros de la UE lo permitiera; en cumplimiento de la Directiva 95/46/CE, las entidades estadounidenses podían adoptar cualquiera de las siguientes posturas: a) adherirse al sistema de Principios de Puerto Seguro; b) acudir a fórmulas que exonerasen del requisito de la protección adecuada, que recoge el artículo 26 de la Directiva 95/46/CE; o, c) no recibir datos de carácter personal de la UE.

9. Ante el incumplimiento por parte de las entidades estadounidenses del sistema de Puerto Seguro, cabían dos posibilidades: a) la suspensión de las transferencias de datos de carácter personal hacia una entidad que haya autocertificado su adhesión a los Principios y su aplicación de conformidad con las *FAQ*, con el fin de proteger a los particulares de un "tratamiento fraudulento" de sus datos de carácter personal, o la adopción de cualquier otra medida dentro de sus competencias con el fin de evitar ese "tratamiento fraudulento" de los datos de carácter personal de los particulares; o, b) si se demostrara que un organismo encargado del cumplimiento de los Principios de Puerto Seguro en los EE.UU. no está ejerciendo su función, la Comisión Europea le notificaría al *US Department of Commerce* que tenía intención de adoptar toda una serie de medidas con el objeto de anular, suspender o restringir la transferencia internacional de datos de carácter personal entre los EE.UU. y la UE.

10. El denominado *Safe Harbour* (Puerto Seguro) por el que se establecía el sistema de Principios de Puerto Seguro para la protección de la vida privada, basado en la voluntaria y libre autocertificación y autoevaluación de las entidades de los EE.UU., tenía como finalidad obtener, respecto de los datos personales recibidos desde la UE una presunción de adecuación a la protección exigida en el ámbito comunitario, que permitiera asegurar, de manera permanente, la legitimidad de las transferencias.

11. En cuanto al ámbito del Acuerdo UE-EE.UU., es preciso especificar varios extremos: a) si se excluían algunos sectores del ámbito del mecanismo de puerto seguro en virtud de disposiciones especiales (por ejemplo, el sector público) o por la inexistencia de un organismo público de supervisión

con responsabilidad para ocuparse de la cuestión; b) si la entidad podría, cuando notificara su adhesión al puerto seguro, excluir algunos sectores de su propia actividad (por ejemplo, los servicios en línea) y cómo se haría pública y se pondría tal exclusión en conocimiento de las autoridades nacionales de control; c) respecto de las transferencias de datos de trabajadores, reforzar el nivel general de protección que brindan los principios o excluir dichos datos del ámbito de aplicación de los acuerdos para proporcionarles mayor protección, en vista asimismo de la inexistencia de un organismo público independiente capaz de ocuparse de este tipo de datos; d) no introducir excepciones a la aplicación de los principios recurriendo a la regulación y sin tomar en la debida cuenta los intereses de la protección de la intimidad.

II. Los principios de *Safe Harbour* o la apuesta por restaurar la confianza en las transferencias internacionales entre los EE.UU. y la UE.: "Scherems I".

12. Así las cosas, a finales de septiembre de 2013, *Safe Harbour* contaba con 3246 empresas adheridas; un aumento muy significativo si lo comparamos con las 400 empresas que había en el año 2004. No obstante, la radiografía era inquietante: había una falta de confianza en las transferencias internacionales de datos entre los EE.UU. y la UE. Razones de seguridad nacional no debían poner en tela de juicio el cumplimiento de los Principios de Puerto Seguro. El funcionamiento de los Principios de Puerto Seguro debió seguir basándose en los compromisos y la autocertificación de las empresas que se han adherido. Los Principios de Puerto Seguro debían seguir actuando como un conducto para la transferencia de los datos personales de los ciudadanos de la UE a los EE.UU. y de las empresas estadounidenses a la UE, en vez de transferirlos a las agencias de inteligencia de EE.UU., en virtud de los programas de vigilancia de los EE.UU.

13. Pero, no fue así: el TJUE declaró inválida la Decisión 2000/520/CE que consideraba que los principios de Puerto Seguro garantizaban un nivel adecuado de protección de los datos transferidos desde la UE a empresas norteamericanas.[1] La sentencia de 6/10/2015 resuelve sobre una cuestión prejudicial planteada por la Corte Suprema irlandesa a raíz de un recurso (caso "Scherems I"- *Maximilliam Schrems vs.* Comisionado de Protección de Datos) interpuesto por un nacional austríaco que entendía que la autoridad de control irlandesa debía prohibir a Facebook Ireland transferir los datos personales de sus usuarios a su matriz estadounidense, Facebook, Inc., debido a que el derecho y las prácticas en vigor de los EE.UU. no garantizaban protección suficiente de los datos personales conservados en su territorio contra l vigilancia practicada en él por las autoridades públicas, haciendo referencia a las revelaciones efectuadas por Snowden sobre las prácticas de la Agencia Nacional de Seguridad.

14. No obstante, el 2 de febrero de 2016, la Comisión Europea y el Gobierno de los EE.UU. alcanzaron un acuerdo político sobre un nuevo marco para los intercambios transatlánticos de datos personales con fines comerciales: el Escudo de la privacidad UE-EE.UU (IP/16/216). La Comisión presentó los textos del proyecto de decisión el 29 de febrero de 2016. Tras el dictamen del Grupo de Trabajo del Artículo 29 (autoridades de protección de datos) de 13 de abril y la Resolución del Parlamento Europeo de 26 de mayo, la Comisión culminó el procedimiento de adopción el 12 de julio de 2016.

15. El Escudo de la privacidad UE-EE.UU reflejaba los requisitos establecidos por el TJUE, en su sentencia de 6 de octubre de 2015, en la que declaraba inválido el antiguo marco de «puerto seguro». El Escudo de la privacidad se basaba en los siguientes principios: a) Obligaciones rigurosas para las empresas que trabajan con datos: al amparo del nuevo sistema, el Departamento de Comercio de los EE.UU. llevará a cabo actualizaciones y revisiones periódicas de las empresas participantes, con el fin de garantizar que sigan las normas que ellas mismas han suscrito. Si las empresas no cumplen en la práctica, se enfren-

[1] *Vid.* F. M. Roselló rubert, "La transferencia de datos personales entre PYMEs españolas y proveedores norteamericanos de *Cloud Computing* tras la reciente anulación del Acuerdo Safe Harbor por el Tribunal de Justicia de la Unión Europea", en *Diario La Ley*, Nº 8725, Sección Doctrina, 18 de Marzo de 2016; Ref. D-115, Editorial LA LEY.

tan a sanciones y a ser retiradas de la lista. El endurecimiento de las condiciones para las transferencias ulteriores de datos a terceros garantizará el mismo nivel de protección en caso de transferencia desde una empresa adherida al Escudo de la privacidad; b) Obligaciones en materia de transparencia y salvaguardias claras para el acceso de la administración estadounidense: los EE.UU. han dado a la UE garantías de que el acceso de las autoridades públicas a efectos de aplicación de la ley y de seguridad nacional está sujeto a limitaciones, salvaguardias y mecanismos de supervisión claros. También por primera vez, cualquier persona en la UE tendrá a su disposición vías de recurso en la materia. Los EE.UU. han descartado una vigilancia masiva indiscriminada de los datos personales transferidos hacia ese país en el marco del acuerdo del Escudo de la privacidad UE-EE UU. La Oficina del Director de Inteligencia Nacional explica además que la recopilación en bloque de datos solo podrá utilizarse en condiciones específicas predeterminadas y tiene que ser lo más concreta y precisa posible. Detalla las salvaguardias existentes para la utilización de los datos en esas circunstancias excepcionales. El secretario de Estado estadounidense ha establecido un mecanismo de recurso en el ámbito de la inteligencia nacional para los europeos a través de la figura del Defensor del Pueblo dentro del Departamento de Estado; c) Protección eficaz de los derechos individuales: cualquier ciudadano que considere que sus datos se han utilizado de forma indebida en el nuevo sistema del Escudo de la privacidad se beneficiarán de varios mecanismos de resolución de litigios accesibles y asequibles. Lo ideal es que las reclamaciones las resuelva la propia empresa; o se ofrecerán gratuitamente mecanismos de resolución alternativa de litigios. Los particulares también podrán dirigirse a sus autoridades nacionales de protección de datos, que colaborarán con la Comisión Federal de Comercio para garantizar que las reclamaciones de los ciudadanos de la UE se investiguen y resuelvan. Si un asunto no se resuelve por un medio u otro, estará previsto, en última instancia, un mecanismo de arbitraje. El mecanismo de recurso en el ámbito de la seguridad nacional para los ciudadanos de la UE será gestionado por un Defensor del pueblo independiente de los servicios de inteligencia de los EE.UU.; y d) Mecanismo de revisión conjunta anual: el mecanismo hará un seguimiento del funcionamiento del Escudo de la privacidad, incluidos los compromisos y garantías en lo que se refiere al acceso a los datos a efectos de aplicación de la ley o de seguridad nacional. La Comisión Europea y el Departamento de Comercio de los EE.UU. llevarán a cabo el examen y asociarán al mismo a expertos nacionales de inteligencia de los EE.UU. y a las autoridades europeas de protección de datos. La Comisión se basará en todas las demás fuentes de información disponibles y presentará un informe público al Parlamento Europeo y al Consejo.

16. En cuanto a los pronunciamientos contenidos en la STJUE "Schrems I" resulta pertinente la realización de un breve análisis de los antecedentes fácticos y jurídicos que nos llevan a la Sentencia objeto de estudio, constituyendo el punto de partida la reclamación que el Sr. Schrems presentó, en fecha 25 de junio de 2013, ante el Comisario, en la que le solicitaba, en esencia, que prohibiera a Facebook Ireland transferir sus datos personales a los EE.UU., alegando el reclamante que el Derecho y las prácticas en vigor en dicho país no garantizaban una protección suficiente de los datos personales conservados en su territorio frente a las actividades de vigilancia llevadas a cabo, en dicho país, por las autoridades públicas. Esta reclamación fue desestimada basándose en que, en particular, la Comisión había declarado, en su Decisión 2000/520/CE de "Puerto Seguro"[2], que los EE.UU. ofrecían un nivel adecuado de protección.

17. La High Court (Tribunal Superior, Irlanda), ante la que el Sr. Schrems había interpuesto un recurso contra la desestimación de su reclamación, planteó al TJUE una petición de decisión prejudicial relativa a la interpretación y a la validez de la Decisión 2000/520/CE, que dio lugar a la Sentencia de 6 de octubre de 2015, que se denominará como "Schrems I", en la que el TJUE declaró inválida la referida Decisión[3].Como consecuencia de dicha Sentencia, el órgano jurisdiccional remitente anuló la desestimación de la reclamación del Sr. Schrems, devolviendo la misma al Comisario.

[2] Decisión de la Comisión, de 26 de julio, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de los EE.UU. de América (DO 2000, L 215, p. 7).

[3] Sentencia del Tribunal de Justicia de 6 de octubre de 2015, Schrems, C-362/14.

18. Cabe señalar que, en el marco de la investigación abierta por este último, Facebook Ireland alegó que una gran parte de los datos personales se transfería a Facebook Inc. basándose en cláusulas tipo de protección de datos recogidas en el anexo de la Decisión 2010/87/UE[4], por lo que, teniendo en cuenta todos estos elementos, el Comisario instó al Sr. Schrems a modificar su reclamación.

19. Atendiendo el requerimiento del Comisario, el Sr. Schrems presentó, el 1 de diciembre de 2015, su reclamación modificada en base a la nuevas circunstancias acaecidas (Sentencia "Schrems I" y alegaciones de Facebook Inc. ante la Comisión, acerca de su actuación conforme a la Decisión 2010/87/UE), alegando, principalmente, que el Derecho estadounidense obliga a Facebook Inc. a poner los datos personales que se le transfieren a disposición de las autoridades estadounidenses, como la National Security Agency (NSA) y la Federal Bureau of Investigation (FBI). La reclamación modificada afirmaba, además, que, al utilizarse esos datos en el marco de diferentes programas de vigilancia, de una manera incompatible con los artículos 7, 8 y 47 de la Carta[5] (que reconocen, respectivamente, el derecho a la vida privada y familiar, el derecho a la protección de datos de carácter personal y el derecho a la tutela judicial efectiva, y a un juez imparcial para la obtención de la tutela de los derechos y libertades reconocidos en el marco de la Unión Europea), la Decisión 2010/87/UE no puede justificar la transferencia de esos datos a los EE.UU. en base a las cláusulas tipo de protección de datos que se recogen en la misma. Teniendo en cuenta estos argumentos, el Sr. Schrems solicitó al Comisario que prohibiese o suspendiese la transferencia de sus datos personales a Facebook Inc.

20. Con posterioridad a la presentación de la reclamación modificada por el Sr. Schrems, el 24 de mayo de 2016, el Comisario publicó un "proyecto de decisión" en el que se resumían las conclusiones provisionales de su investigación. En dicho proyecto, consideró con carácter provisional que los datos personales de ciudadanos de la Unión Europea transferidos a EE.UU. corrían el riesgo de ser consultados y tratados por las autoridades estadounidenses de una manera incompatible con los artículos 7 y 8 de la Carta y que el Derecho estadounidense no ofrece a esos ciudadanos vías de recurso compatibles con el artículo 47 de la Carta. El Comisario estimó que las cláusulas tipo de protección de datos recogidas en el anexo de la Decisión CPT no subsanan esa deficiencia, en la medida en que sólo confieren a los interesados derechos contractuales contra el exportador o el importador de los datos, sin vincular a las autoridades estadounidenses.

21. De esta forma, al considerar que, en esas circunstancias, la reclamación modificada del Sr. Schrems planteaba la cuestión de la validez de la Decisión 2010/87/UE relativa a cláusulas contractuales tipo, el 31 de mayo de 2016, el Comisario inició un procedimiento ante la High Court (Tribunal Superior), apoyándose en la jurisprudencia resultante de la sentencia "Schrems I", de 6 de octubre de 2015, apartado 65, a efectos de que esta última pregunte al TJUE acerca de esta cuestión. Mediante resolución de 4 de mayo de 2018, la High Court (Tribunal Superior) planteó la petición de decisión prejudicial ante el TJUE que, finalmente, se resuelve por la Sentencia "Schrems II".

---

[4] 2010/87/UE: Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

[5] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 7: "Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones." Artículo 8: "Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán 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. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente." Artículo 47: "Derecho a la tutela judicial efectiva y a un juez imparcial. Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia."

22. Es conveniente resaltar que, durante todo este *iter* procedimental se producen dos hechos que constituyen antecedentes a tener en cuenta. La primera de las circunstancias ocurridas durante toda la tramitación someramente reproducida es que, con posterioridad a la declaración de invalidez de la Decisión "Puerto seguro", por la Sentencia "Schrems I", la Comisión adoptó la Decisión "Escudo de Privacidad"[6] que tenía como vocación ocupar el vacío dejado por la declaración de invalidez contenida en la referida Sentencia, constituyendo su validez, como se verá, uno de los puntos fundamentales de la Sentencia que es objeto de análisis en el presente estudio. La segunda de estas circunstancias con cierta relevancia para el análisis de la cuestión objeto del presente trabajo, es la entrada en vigor del RGPD, que sustituyó a la Directiva 95/46/CE, manteniendo, no obstante, en lo sustancial, la regulación contenida en ésta sobre la transferencia de datos personales a terceros países extracomunitarios.

23. Con respecto a esta última circunstancia, considera el Tribunal que aunque las cuestiones prejudiciales planteadas se refieren a las disposiciones de la Directiva 95/46/CE, deberán responderse en base al RGPD, ya que el Comisario aún no había adoptado una decisión final sobre esa reclamación cuando la Directiva fue derogada y sustituida por el RGPD, con efecto a partir del 25 de mayo de 2018, por lo que es esta norma, y no la Directiva derogada, la que toma en consideración el Tribunal para la resolución de las cuestiones prejudiciales planteadas.

III. Un nuevo esfuerzo (baldío) por restaurar la confianza en las transferencias internacionales entre los EE.UU. y la UE.: "Scherems II"

24. La STJUE, de 16 de julio de 2020, dictada en el Asunto C-311/18, (en adelante, Sentencia "Schrems II") constituye un hito esencial en una sucesión de hechos relacionados con una de las cuestiones que mayor debate ha generado en los últimos años en materia de protección de datos, como es la transferencia de datos personales protegidos por el Derecho de la Unión a terceros países extracomunitarios, especialmente, a los EE.UU. de América.

25. Se trata de una cuestión cuya suma importancia resulta comprensible en un mundo en el que la globalización alcanza su máximo exponente en el campo de los datos personales protegidos, principalmente, debido a la existencia de redes sociales u otras plataformas digitales que operan a nivel mundial tratando datos personales protegidos de sus usuarios que, en muchos casos, se refieren a la esfera más íntima de su privacidad.

26. Esta situación es de enorme importancia por cuanto que, de no establecerse los adecuados criterios de control del respeto a la normativa comunitaria en materia de protección de datos de carácter personal, en este tipo de transferencias a terceros países extracomunitarios, nos encontraríamos con que la protección de datos de carácter personal quedarían limitados a un ámbito territorial relativamente reducido, con lo que los ciudadanos de la Unión Europea estarían desprotegidos en multitud de ocasiones en los que sus datos personales serán tratados en países ajenos al territorio comunitario.

27. Es por ello por lo que, la normativa comunitaria de protección de datos de carácter personal, representada en la actualidad por el RGPD establece unos criterios reguladores de dichas transferencias a países extracomunitarios, con la evidente finalidad de mantener, aún en estos casos, el debido nivel de protección de los datos de carácter personal de los ciudadanos de la Unión.

[6] 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 Privacidad UE-EEUU (DO 2016, L 207, p.1).

28. De esta forma, a grandes rasgos, el RGPD establece un mecanismo de protección que se configura en tres niveles, debiendo considerarse, en primer lugar, lo establecido en su artículo 45[7], que regula la emisión de Decisiones de Adecuación por parte de la Comisión; en segundo lugar, lo dispuesto por su artículo 46, que establece un sistema de garantías sostenido, principalmente, por las normas corporativas vinculantes y las cláusulas tipo de protección de datos. Por último, lo dispuesto en su artículo 49 que, en defecto de los mecanismos dispuestos en los anteriores preceptos, establece una serie de supuestos relacionados taxativamente, en los que pueden realizarse transferencias de datos a terceros países comunitarios, que descansan, en general, en el expreso consentimiento del interesado, previa advertencia de los riesgos de la transferencia de sus datos, así como en razones de interés general que, en cualquier caso, deberán respetar las garantías del derecho Comunitario.

29. Teniendo en cuenta lo anterior, la Sentencia "Schrems II" es de enorme importancia por cuanto que, a pesar de referirse a las transferencias de datos personales protegidos a los EE.UU., establece con nitidez los parámetros que deberán ser tenidos en cuenta para las transferencias de datos a terceros países extracomunitarios, definiendo con claridad conceptos esenciales como es el nivel de protección adecuado de los datos personales que ha de ser tomado en consideración, o las obligaciones y

[7] Artículo 45 del RGPD: "Transferencias basadas en una decisión de adecuación. 1. 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. Dicha transferencia no requerirá ninguna autorización específica. 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) 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, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) 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 interesados 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. 3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. 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. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2. 4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE. 5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2. Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3. 6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5. 7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49. 8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado. 9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo".

facultades, tanto de las autoridades públicas de control, como de todos los sujetos implicados en la transferencia y tratamiento de datos personales protegidos con destino a terceros países extracomunitarios.

30. Por esta razón, a pesar de que el objeto y alcance de la Sentencia "Schrems II" puede parecer limitado al caso de los EE.UU., lo cierto es que la misma ha marcado un antes y un después en las transferencias extracomunitarias de datos de carácter personal al definir elementos esenciales para garantizar que los derechos de los ciudadanos de la Unión Europea, afectados por estas transferencias, no quedan desprotegidos.

31. Estamos ante una cuestión enormemente importante, que hará correr ríos de tinta, por lo que, es evidente que, no llegaremos a alcanzar, en el presente trabajo, todas las implicaciones y matices que tiene la Sentencia. Sin perjuicio de ello, no cabe duda del interés jurídico del presente estudio, en el que se partirá de un breve relato de los antecedentes que nos han conducido a este hito, concretando el objeto de la cuestión prejudicial planteada, para llegar al concreto análisis de la decisión que, el TJUE, ha alcanzado con respecto a cada una de estas cuestiones controvertidas.

32. Aunque el órgano judicial nacional formula un total de once cuestiones prejudiciales, el Tribunal agrupa sistemáticamente las mismas de manera que el objeto de decisión se reduce a cinco cuestiones que se relacionarán a continuación.

33. La primera cuestión prejudicial, tiene como objeto la determinación de la inclusión dentro del ámbito de aplicación del RGPD de las transferencias de datos personales realizada por un operador económico establecido en un Estado miembro, a otro operador económico establecido en un país tercero cuando, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado.

34. El segundo grupo sistemático de la reclamación prejudicial formulada, en el que el Tribunal incluye las cuestiones prejudiciales segunda, tercera y sexta, es de suma importancia, por cuanto que se traduce en la delimitación de los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garantizado en el contexto de una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos.

35. En tercer lugar, el TJUE se pronuncia sobre la cuestión prejudicial octava, que se refiere a la determinación de las facultades de las autoridades de control competentes y, concretamente, a si éstas están obligadas a suspender o prohibir una transferencia de datos personales a un país tercero, que esté basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando por parte de la correspondiente autoridad de control se considera que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero.

36. El cuarto grupo sistemático objeto de resolución por la STJUE "Schrems II" comprende las cuestiones prejudiciales séptima y undécima, concretándose en el análisis de la validez de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo, bajo el prisma de la Carta de Derechos Fundamentales de la UE.

37. En quinto y último lugar, se valoran por el Tribunal, de forma conjunta, las cuestiones prejudiciales cuarta, quinta, novena y décima que, en suma, se refieren a una cuestión de vital importancia como es la validez de la Decisión "Escudo de Privacidad", así como el grado de garantía de la tutela judicial efectiva que, para los ciudadanos de la UE, ofrece la figura del Defensor del Pueblo mencionado en el Anexo III de la referida Decisión.

IV. La Sentencia "Schrems II"

1. Sobre el ámbito de aplicación del RGPD

38. Como se ha expuesto, el objeto de la primera cuestión prejudicial se concreta en la inclusión, dentro del ámbito de aplicación del RGPD de una transferencia de datos personales realizada por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero cuando, en el transcurso de esa transferencia o tras ella, esos datos puedan ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado.

39. El Tribunal resuelve esta cuestión considerando que este tipo de transferencias se encuentran dentro del ámbito de aplicación del RGPD, tras un acertado análisis del ámbito de aplicación del mismo, conforme a lo dispuesto en su artículo 2, apartado 1, que establece que el RGPD se aplica al tratamiento total, o parcialmente automatizado, de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Toma en consideración, también, el Tribunal la definición que el artículo 4, punto 2 del RGPD, realiza del concepto de "tratamiento" como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no", así como los ejemplos que, de dicho concepto, se citan en el referido precepto, como es la "comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso", debiendo tenerse en cuenta, además, a juicio del Tribunal, que el referido RGPD aplica, a las transferencias de datos personales a países terceros, normas particulares recogidas en su capítulo V, titulado "Transferencias de datos personales a terceros países u organizaciones internacionales", y confiere a las autoridades de control poderes específicos a ese efecto, que se recogen en el artículo 58[8], apartado 2, letra j), del RGPD.

40. No existiendo dudas con respecto a que el RGPD se aplica a las transferencias de datos personales a países terceros extracomunitarios, pasa el Tribunal a analizar si, el supuesto de hecho de la cuestión prejudicial planteada resulta incardinable a alguna de las excepciones que establece el Reglamento en cuanto a su ámbito de aplicación establecidas en el artículo 2[9], apartado 2 del RGPD que, como recuerda el TJUE, deben interpretarse en sentido estricto[10].

41. Así las cosas, el Tribunal concluye que, en el caso de autos, al haber sido realizada la transferencia de datos personales que es objeto del litigio principal, por Facebook Ireland hacia Facebook Inc., es decir, entre dos personas jurídicas, dicha transferencia no está comprendida dentro del ámbito del artículo 2, apartado 2, letra c) del RGPD, que tiene por objeto el tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. A la referida transferencia tampoco pueden aplicársele las excepciones recogidas en el artículo 2[11], apartado 2, letras a), b) y d), del antedicho Reglamento, ya que las actividades que allí se enumeran a título de ejemplo

[8] Artículo 58, apartado 2, letra j) del RGPD: "Poderes. Ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional."

[9] Artículo 2, apartado 2 del RGPD: "Ámbito de aplicación material 2. El presente Reglamento no se aplica al tratamiento de datos personales: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."

[10] *Vid*. en lo que se refiere al artículo 3, apartado 2, de la Directiva 95/46/CE, la sentencia de 10 de julio de 2018, Jehovan todistajat, C25/17, EU:C:2018:551, apartado 37 y jurisprudencia citada).

[11] Artículo 2, apartado 2, letras a), b) y d) del RGPD: "Ámbito de aplicación material: a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión; b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE; d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención."

son, en todos los casos, actividades propias del Estado o de las autoridades estatales y ajenas a la esfera de actividades de los particulares.

42. Por todo ello concluye el Tribunal, con respecto a la primera de las cuestiones prejudiciales planteadas, que la posibilidad de que los datos personales transferidos entre dos operadores económicos con fines comerciales sean objeto, en el transcurso de la transferencia o tras ella, de un tratamiento con fines de seguridad pública, defensa o seguridad del Estado por parte de las autoridades del país tercero de que se trate, no puede excluir a la referida transferencia del ámbito de aplicación del RGPD.

2. Sobre el nivel de protección adecuado para la transferencia de datos a terceros países

43. Como se ha avanzado, el segundo grupo de cuestiones analizadas por el TJUE, se centra en la delimitación de los elementos que han de tomarse en consideración a efectos de determinar si ese nivel de protección está garantizado en el contexto de una transferencia de datos personales a un país tercero basada en cláusulas tipo de protección de datos.

44. En relación con esta cuestión, analiza el TJUE, en primer lugar, lo dispuesto por el artículo 46[12], apartados 1 y 2, letra c) del RGPD, tras una lectura conjunta de esas disposiciones, concluyendo que, cuando no existe una decisión de adecuación adoptada en virtud del artículo 45[13], apartado 3, del referido Reglamento, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país si hubiera ofrecido "garantías adecuadas", siempre que se cumpla la condición de que los interesados cuenten "con derechos exigibles y acciones legales efectivas", pudiendo proporcionarse esas garantías adecuadas, en particular, mediante cláusulas tipo de protección de datos adoptadas por la Comisión.

45. Afirma el Tribunal que el artículo 45[14], apartado 1, primera frase del RGPD establece que podrá autorizarse una transferencia de datos personales a un tercer país mediante una decisión adoptada por la Comisión, conforme a la cual se atestigua que ese tercer país, un territorio o uno o varios sectores específicos de ese tercer país garantizan un nivel de protección adecuado. A este respecto, sin exigir que el país tercero de que se trate garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión Europea, debe entenderse que la expresión "nivel de protección adecuado", tal como queda confirmado en el considerando 104 del referido Reglamento, exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y de los derechos fundamentales sustancialmente equivalente al garantizado en

[12] Artículo 46, apartados 1 y 2, letra c) del RGPD: "Transferencias mediante garantías adecuadas 1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. 2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por: 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."

[13] Artículo 45, apartado 3 del RGPD: "Transferencias basadas en una decisión de adecuación. 3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. 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. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2."

[14] Artículo 45, apartado 1 del RGPD: "Transferencias basadas en una decisión de adecuación 1. 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. Dicha transferencia no requerirá ninguna autorización específica."

la Unión Europea en virtud del antedicho Reglamento, interpretado a la luz de la Carta. En efecto, a falta de esa exigencia, el objetivo mencionado en el anterior apartado se frustraría[15].

46. En este sentido, concluye el Tribunal que las garantías adecuadas deben asegurar que las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gocen, como en el marco de una transferencia basada en una decisión de adecuación, de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión.

47. En relación con el marco sobre el que ha de interpretarse el alcance del nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea, analiza el Tribunal si el análisis del nivel de protección debía determinarse a la luz del Derecho de la Unión, en particular, de los derechos garantizados por la Carta y/o a la luz de los derechos fundamentales reconocidos en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, o también a la luz del Derecho nacional de los Estados miembros. Con respecto a esta cuestión, concluye el Tribunal que el nivel de protección de los derechos fundamentales exigido en el artículo 46, apartado 1, del antedicho Reglamento debe determinarse sobre la base de las disposiciones del mismo Reglamento, interpretadas a la luz de los derechos fundamentales garantizados por la Carta.

48. Por último, determina el Tribunal los elementos que han de tomarse en consideración para determinar la adecuación del nivel de protección en el contexto de una transferencia de datos personales a un país tercero sobre la base de las cláusulas tipo de protección de datos adoptadas en virtud del artículo 46, apartado 2, letra c) del RGPD, respondiendo el Tribunal que han de tenerse en cuenta, por una parte, las estipulaciones contractuales objeto de acuerdo entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate y, por otra parte, en lo que respecta al hipotético acceso de las autoridades públicas del país tercero, a los datos personales transferidos, se han de tener en cuenta los elementos mencionados, de modo no exhaustivo, en el artículo 45, apartado 2 del RGPD, que precisa que los interesados deben gozar de garantías adecuadas y contar con derechos exigibles y acciones legales efectivas.

49. Por tanto, teniendo en cuenta todo lo anterior, el Tribunal interpreta el nivel de protección adecuado para la transferencia de datos a terceros países en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas por dichas disposiciones deben garantizar que los derechos de las personas cuyos datos personales se transfieren a un país tercero sobre la base de cláusulas tipo de protección de datos gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión Europea por el referido Reglamento, interpretado a la luz de la Carta. A tal efecto, la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características debe, en particular, tomar en consideración tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión Europea y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el artículo 45[16], apartado 2 del RGPD.

---

[15] *Vid.*, en lo que respecta al artículo 25, apartado 6, de la Directiva 95/46, la sentencia de 6 de octubre de 2015, Schrems, C362/14, EU:C:2015:650, apartado 73.

[16] Artículo 45, apartado 2 del RGPD: "Transferencias basadas en una decisión de adecuación. 2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) 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, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control

3. Sobre las obligaciones de control de las autoridades

50. Como se ha visto, el TJUE analiza, de forma independiente, la cuestión prejudicial octava, que se refiere a la determinación de las facultades de las autoridades de control competentes y, concretamente, a si éstas están obligadas a suspender o prohibir una transferencia de datos personales a un país tercero, basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando por parte de la correspondiente autoridad de control se considera que dichas cláusulas no se respetan, o no pueden respetarse en ese país tercero, así como que la protección de los datos transferidos exigida por el Derecho de la Unión Europea, en particular, por los artículos 45 y 46 del RGPD y por la Carta, no puede garantizarse, o si, por el contrario, el ejercicio de esas facultades de suspensión o prohibición de las transferencias están limitadas a supuestos excepcionales[17].

51. Esta cuestión prejudicial es resuelta por el mencionado Tribunal en el sentido de considerar dos escenarios diferentes dependiendo de la existencia o no de una decisión de adecuación dictada por la Comisión. En el caso de que exista una decisión de adecuación, y mientras que la misma no haya sido objeto de invalidación por el TJUE, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciará con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado ni, por consiguiente, suspender o prohibir transferencias de datos personales a ese tercer país.

52. No obstante, aclara el Tribunal que incluso habiendo adoptado la Comisión una decisión de adecuación, la autoridad nacional de control competente, a la que una persona haya presentado una reclamación para proteger sus derechos y libertades frente al tratamiento de datos personales que la conciernen, debe poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por el RGPD y, en su caso, interponer un recurso ante los tribunales nacionales, para que estos, si concuerdan en las dudas de esa autoridad sobre la validez de la decisión de adecuación, planteen al TJUE una cuestión prejudicial sobre esta validez[18].

53. Por el contrario, en el caso de que no exista una decisión de adecuación emitida por la Comisión, el Tribunal resuelve que la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control considera, a la luz de todas las circunstancias específicas de la referida transferencia, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión Europea, en particular, por los artículos 45 y 46[19] del RGPD y por la Carta, no puede garantizarse mediante otros

---

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 interesados 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."

[17] *Vid.*, en relación con la traslación de la responsabilidad hacia el responsable del tratamiento, J.F. RODRÍGUEZ AYUSO, "Anulación del Privacy Shield en las transferecnias internacionales de datos: ¿presenciamos un desplazamiento fáctico de la responsabilidad?", en *Revista Boliviana de Derecho*, Nº 31, enero 2021, pp. 426-503.

[18] *Vid.*, en lo que respecta al artículo 25, apartado 6, y al artículo 28 de la Directiva 95/46/CE, la sentencia de 6 de octubre de 2015, Schrems, C362/14, EU:C:2015:650, apartado 57 y 65.

[19] Artículo 46 del RGPD: "Transferencias mediante garantías adecuadas. 1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. 2. 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,

medios, en especial si el responsable o el encargado del tratamiento establecidos en la Unión Europea no han suspendido la transferencia o puesto fin a esta por sí mismos.

4. Sobre la validez de la Decisión 2010/87/UE

54. Como se ha señalado, el cuarto grupo sistemático objeto de resolución por la Sentencia "Schrems II" comprende las cuestiones prejudiciales séptima y undécima que, en esencia, tratan sobre el análisis de la validez de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo bajo el prisma de la Carta de Derechos Fundamentales de la Unión Europea.

55. El TJUE hace depender la validez de la Decisión 2010/87/UE a si, de conformidad con la exigencia resultante de los artículos 46, apartado 1 y 2, letra c), del RGPD, interpretados a la luz de los artículos 7, 8 y 47 de la Carta[20], tal decisión incluye mecanismos efectivos que permitan, en la práctica, garantizar que el nivel de protección exigido por el Derecho de la Unión Europea sea respetado, así como que las transferencias de datos personales basadas en esas cláusulas sean suspendidas o prohibidas en caso de violación de dichas cláusulas, o de que resulte imposible su cumplimiento.

56. El referido Tribunal analiza los concretos mecanismos efectivos de protección de datos que se recogen en el anexo de la Decisión 2010/87/UE concluyendo que, de las cláusulas 4, letras a) y b), 5, letra a), 9 y 11, apartado 1, de dicho anexo se desprende que el responsable del tratamiento establecido en la Unión Europea, el destinatario de la transferencia de datos personales y el eventual encargado de este último, se comprometen mutuamente a que el tratamiento de esos datos, incluida su transferencia, ha sido efectuado y seguirá efectuándose de conformidad con la legislación de protección de datos aplicable, que, conforme al artículo 3, letra f) de la antedicha Decisión se corresponde con la legislación que protege los derechos y libertades fundamentales de las personas y, en particular, su derecho a la vida privada respecto del tratamiento de los datos personales, aplicable al responsable del tratamiento en el Estado miembro en que está establecido el exportador de datos.

---

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 tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados. 3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados. 4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo. 5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo."

[20] Carta de los Derechos Fundamentales de la Unión Europea. Artículo 7: "Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones." Artículo 8: "Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán 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. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente." Artículo 47: "Derecho a la tutela judicial efectiva y a un juez imparcial. Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia."

57. Asimismo, se analizan por el TJUE las obligaciones del destinatario de la transferencia de datos personales establecido en un país tercero, que se concretan en una información inmediata, al responsable del tratamiento establecido en la Unión Europea, de su eventual incapacidad para cumplir con las obligaciones que le incumben con arreglo al contrato celebrado, teniendo la posibilidad, en este caso, el responsable del tratamiento establecido de suspender la transferencia de los datos o rescindir el contrato interpretando el TJUE que esta facultad es obligatoria para el responsable del tratamiento cuando el destinatario de la transferencia establecido en un país extracomunitario no cumple, o ya no puede cumplir, las cláusulas tipo de protección de datos, por lo que, más que una facultad, se convierte en una obligación del responsable de tratamiento establecido en la Unión Europea.

58. Por tanto, concluye el TJUE que la interpretación de los mecanismos incluidos en la Decisión 2010/87/UE, obligan al responsable del tratamiento establecido en la Unión Europea y al destinatario de la transferencia de datos personales a asegurarse de que la legislación del país tercero de destino permita al antedicho destinatario cumplir con las cláusulas tipo de protección de datos recogidas en la propia Decisión 2010/87/UE, antes de llevar a cabo una transferencia de datos personales a ese país tercero.

59. En lo que se refiere al alcance de dicha comprobación a efectuar por los sujetos intervinientes en la transferencia de datos, o lo que es lo mismo, cuando debe considerarse por éstos que la legislación del país extracomunitario es incompatible con las cláusulas, señala el TJUE que, las obligaciones impuestas por esa legislación que no vayan más allá de las restricciones necesarias en una sociedad democrática para la salvaguardia, en particular, de la seguridad del Estado, la defensa y la seguridad pública no están en contradicción con las cláusulas tipo de protección de datos, por lo que, *sensu* contrario, el hecho de acatar una obligación dictada por el Derecho del país tercero de destino que vaya más allá de lo necesario para la consecución de tales fines debe considerarse una violación de las antedichas cláusulas.

60. Conforme a lo establecido en el anexo de la Decisión 2010/87/UE, el responsable del tratamiento establecido en la Unión Europea está obligado, cuando el destinatario de la transferencia de datos personales le notifica, que la legislación que le es de aplicación ha sido objeto de una modificación que puede tener un importante efecto negativo sobre las garantías ofrecidas y las obligaciones impuestas por las cláusulas tipo de protección de datos, a enviar esa notificación a la autoridad de control competente en caso de que, a pesar de dicha notificación por parte del destinatario establecido en el país extracomunitario, el responsable de tratamiento establecido en la Unión Europea, decida proseguir la transferencia, o levantar una suspensión previamente acordada. El envío de la referida notificación a la autoridad de control competente, y la facultad de ésta de auditar al destinatario de la transferencia de datos personales, permiten a la mencionada autoridad de control comprobar si es preciso proceder a la suspensión o la prohibición de la transferencia prevista para garantizar un nivel de protección adecuado.

61. Por lo tanto, advierte el Tribunal que, incluso teniendo en cuenta las obligaciones de notificación e información del destinatario extracomunitario, y la obligación de suspensión o finalización de la transferencia de datos por parte del responsable del tratamiento las partes, en el caso de que éste decida no suspender o no finalizar la transferencia, tiene una obligación de notificación a la autoridad de control competente que podrá suspender o prohibir, en su caso, una transferencia de datos personales a un país tercero basada en las cláusulas tipo de protección de datos recogidas en el anexo de dicha Decisión 2010/87/UE, debiendo la autoridad de control ejercer las facultades que le corresponden conforme a lo resuelto en la propia Sentencia "Schrems II".

62. Por todo lo expuesto, concluye el TJUE que la Decisión 2010/87/UE prevé mecanismos efectivos que permiten, en la práctica, garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas, incluyendo la posibilidad de control por las autoridades en el caso de

que por el responsable del tratamiento no se suspenda o prohíba la transferencia, por lo que entiende que no se presenta ningún elemento que pueda afectar a la validez de dicha Decisión.

5. Sobre la validez de la Decisión "Escudo de Privacidad"

63. Por último, el TJUE entra a valorar la validez de la Decisión "Escudo de Privacidad", atendiendo a si el Derecho de los EE.UU. garantiza efectivamente el nivel de protección adecuado exigido en el artículo 45 del RGPD, interpretado a la luz de los derechos fundamentales garantizados en los artículos 7, 8 y 47 de la Carta teniendo en cuenta que, el órgano jurisdiccional que plantea la cuestión prejudicial considera que el Derecho de los EE.UU. no prevé las limitaciones y garantías necesarias con respecto a las injerencias autorizadas por su normativa nacional, así como que tampoco garantiza una tutela judicial efectiva a los interesados, contra tales injerencias, sin que el mecanismo del Defensor del Pueblo previsto ofrezca la debida protección a la tutela judicial efectiva.

64. Partiendo de este planteamiento se analiza por parte del TJUE la validez de la Decisión "Escudo de Privacidad" teniendo en cuenta, por una parte, la incidencia que las injerencias de las autoridades de EE.UU., conforme al Derecho de aquel país, tiene en el nivel de protección adecuado y, por otra, la validez de la figura de Defensor del Pueblo regulado por la Decisión "Escudo de Privacidad" para garantizar la tutela judicial efectiva de los ciudadanos comunitarios en defensa de sus datos personales protegidos.

65. Con respecto a la primera de las cuestiones, considera el Tribunal que las injerencias resultantes de los programas de vigilancia basados en la FISA[21] y en la E.O. 12333[22] no están sujetas a exigencias que garanticen, un nivel de protección sustancial, considerando el TJUE que las limitaciones que establecen las referidas normas de los EE.UU. no respetan el principio de proporcionalidad, que establece básicamente que las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario.

66. En este sentido, añade el TJUE que la comunicación de datos de carácter personal a un tercero, como una autoridad pública, constituye una injerencia en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta (derecho al respeto a la vida privada y familiar, así como derecho a la protección de datos personales), cualquiera que sea la utilización posterior de la información comunicada, considerando una injerencia similar la conservación de los datos de carácter personal y del acceso a esos datos con vistas a su utilización por parte de las autoridades públicas, con independencia de que la información relativa a la vida privada de que se trate tenga o no carácter sensible o de que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia[23].

67. Aunque el TJUE pone de manifiesto que los anteriores derechos no gozan de carácter absoluto, incide en que cualquier limitación de los mismos, derivada del tratamiento de datos de carácter personal, debe realizarse para fines concretos, sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto en la Ley, que deberá definir con absoluta claridad el alcance de la limitación prevista en los derechos y libertades, estableciendo reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular,

[21] Foreign Intelligence Surveillance Act of 1978 (Ley de Vigilancia de la Inteligencia Extranjera) (*Pub.L.* 95–511, 92 Stat. 1783, 50 U.S.C. cap. 36).

[22] Executive Order 12333.

[23] Se remite el Tribunal de Justicia de la Unión Europea, en este punto a las sentencias de 20 de mayo de 2003, Österreichischer Rundfunk y otros, C465/00, C138/01 y C139/01, EU:C:2003:294, apartados 74 y 75; de 8 de abril de 2014, Digital Rights Ireland y otros, C293/12 y C594/12, EU:C:2014:238, apartados 33 a 36, y el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 124 y 126.

dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario ya que, de lo contrario, no se respetaría el citado principio de proporcionalidad.

68. En el caso objeto de la Sentencia "Schrems II", el TJUE advierte que las injerencias resultantes de los programas de vigilancia basados en la FISA y en la E.O. 12333 exceden de los límites impuestos por la normativa europea de protección de datos de carácter personal, principalmente debido a que los programas de vigilancia autorizados por la normativa de los EE.UU. no se fundamentan en una vigilancia individual sino en programas de vigilancia masivos e indiscriminados y, en definitiva, ilimitados, basados en sistemas de recopilación "en bloque" de los datos personales protegidos que, evidentemente, exceden notablemente de las exigencias de concreción y determinación del alcance de la limitación de los derechos y libertades que derivan del principio de proporcionalidad, por lo que, concluye el Tribunal, que no puede considerarse que los programas de vigilancia basados en esas disposiciones se limiten a lo estrictamente necesario.

69. Con respecto a la segunda de las cuestiones, es decir, sobre la debida garantía del derecho a la tutela judicial efectiva de los interesados, y sobre si la figura del Defensor del Pueblo a la que se refiere la Decisión "Escudo de Privacidad" garantiza este derecho, el TJUE recuerda que el primer párrafo del referido artículo 47 de la Carta requiere que toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión Europea hayan sido violados tenga derecho a la tutela judicial efectiva respetando las condiciones establecidas en el mencionado artículo. A tenor del párrafo segundo del antedicho artículo, toda persona tiene derecho a que su causa sea oída por un juez independiente e imparcial, lo que hace necesaria, en todo caso, la existencia de recursos administrativos y acciones judiciales que sean efectivos y accesibles para las personas cuyos datos personales son objeto de tratamiento.

70. En el caso de autos, la constatación contenida en la Decisión "Escudo de Privacidad", según la cual los EE.UU. garantizan un nivel de protección sustancialmente equivalente al previsto en el artículo 47 de la Carta, fue puesta en entredicho basándose, en particular, en que la creación del Defensor del Pueblo en el ámbito del "Escudo de Privacidad" no puede subsanar las lagunas en lo que respecta a la tutela judicial de las personas cuyos datos personales son transferidos a ese país tercero, considerando el TJUE que esta exigencia no se cumple en este caso, por cuanto la normativa de los EE.UU., en especial en los casos de programas de vigilancia basados en la E.O. 12333, no ofrecen ninguna vía de recurso, por lo que no garantizan la debida tutela judicial efectiva para los ciudadanos cuyos datos son objeto de tratamiento.

71. Entiende el TJUE que la existencia del mecanismo del Defensor del Pueblo no subsana las limitaciones al derecho a la tutela judicial efectiva, poniendo en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo de los EE.UU. y su facultad para emitir decisiones vinculantes para las autoridades estadounidenses sin que, además, constata que no existe ninguna garantía legal que pueda ser invocada por los ciudadanos ante dicho Defensor del Pueblo, por lo que no se cumple con la exigencia de una vía de recurso efectivo garante del derecho a la tutela judicial efectiva en materia de protección de datos.

72. Por lo tanto, concluye el TJUE que la Comisión, al declarar, en el artículo 1, apartado 1, de la Decisión "Escudo de Privacidad", que los EE.UU. garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea a entidades establecidas en ese país tercero en el marco del Escudo de la Privacidad UEEE. UU., no tuvo en cuenta las exigencias resultantes del artículo 45, apartado 1, del RGPD, interpretado a la luz de los artículos 7, 8 y 47 de la Carta por lo que declara la invalidez de dicha Decisión.

73. Por último, se pronuncia el TJUE sobre si es preciso mantener los efectos de la antedicha Decisión "Escudo de Privacidad" para evitar la creación de un vacío legal, concluyendo que en este caso

no se produce tal vacío legal por cuanto que teniendo en cuenta el artículo 49 del RGPD, que establece, de manera precisa, las condiciones en las que pueden tener lugar transferencias de datos personales a países terceros en ausencia de una decisión de adecuación en virtud del artículo 45, apartado 3, del referido Reglamento o de garantías adecuadas con arreglo al artículo 46 del mismo Reglamento.

V. El nuevo marco transatlántico de privacidad de datos

1. Contexto

74. El nuevo Marco de Privacidad de Datos UE-EE.UU. introduce nuevas garantías vinculantes al objeto de dar respuesta a cada uno de los motivos de inquietud puestos de manifiesto, en su día, por el TJUE. Entre estas garantías se encuentran la limitación del acceso por parte de los servicios de inteligencia estadounidenses a los datos de la UE (a lo necesario y proporcionado), y el establecimiento de un Tribunal de Recurso en Materia de Protección de Datos, al que los ciudadanos de la UE tendrán acceso. El nuevo marco introduce mejoras importantes respecto al mecanismo que existía en virtud del *Safe Harbour* o del Escudo de la privacidad. Por ejemplo, si el Tribunal de Recurso en Materia de Protección de Datos concluye que se han recogido datos en contravención de las nuevas garantías, podrá requerir la supresión de los mismos.

75. Las empresas estadounidenses podrán adherirse al Marco de Privacidad de Datos UE-EE.UU. si se comprometen a cumplir una serie de obligaciones detalladas de privacidad; por ejemplo, el requisito de borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida, y a garantizar la continuidad de la protección en caso de compartir los datos de carácter personal con terceros. Y, en caso de tratamiento indebido de sus datos por parte de las empresas estadounidenses, los ciudadanos de la UE se beneficiarán de varias vías de reparación, entre ellos mecanismos de resolución independiente y gratuita de controversias, y un tribunal arbitral. Además, el marco jurídico estadounidense establece una serie de **garantías relativas al acceso por parte de las administraciones públicas estadounidenses** a los datos transferidos al amparo del marco se limita a lo estrictamente necesario: en particular, a efectos penales y de seguridad nacional y sólo en aras a proteger la seguridad nacional.

76. En cuestiones relacionadas con la recogida y el uso de sus datos por parte de los servicios de inteligencia estadounidenses, los ciudadanos de la UE tendrán acceso a unos **órganos independientes e imparciales de impugnación**, entre ellos, como hemos señalado, el nuevo Tribunal de Recurso en Materia de Protección de Datos, que investigará y resolverá las reclamaciones de forma independiente y podrá imponer medidas reparatorias de fuerza vinculante.

77. Un elemento esencial del marco jurídico estadounidense que consagra estas garantías es el Decreto Presidencial de los EE.UU. titulado "Refuerzo de las garantías en las actividades de inteligencia de señales de los EE.UU.", que da respuesta a las reservas manifestadas por el TJUE en su sentencia "Schrems II"[24].

78. A pesar de que no existe legislación federal en materia de privacidad y protección de datos en los EE.UU., son notables los esfuerzos realizados por los EE.UU. en el Decreto nº 14086, introduce definiciones de conceptos fundamentales de la protección de datos, como los principios de necesidad y proporcionalidad, y supone un importante paso adelante con respecto a mecanismos de transferencia anteriores, para fijar límites a las actividades de inteligencia de señales de los EE.UU. haciendo que los

[24] *Vid.* A. Ortega giménez, "A la tercera va la vencida": el nuevo Marco Trasatlántico de Privacidad de Datos EE.UU.-EU (Privay Shield 2.0)", en *LA LEY Privacidad*, Número 14, Editorial Wolters Kluwer, Las Rozas (Madrid), octubre-diciembre 2022, pp. 1-7.

principios de proporcionalidad y necesidad sean aplicables al marco jurídico estadounidense en materia de inteligencia de señales e incorporando una lista de objetivos legítimos para dichas actividades.

79. Si bien el citado Decreto prevé importantes mejoras destinadas a garantizar que estos principios sean sustancialmente equivalentes a los contemplados en el Derecho de la UE, estos principios son desde hace tiempo elementos clave del régimen de protección de datos de la UE y sus definiciones sustantivas recogidas en el Decreto nº 14086 no están en consonancia con su definición en el Derecho de la UE y su interpretación por parte del TJUE.

80. En la medida en que el Decreto nº 14086 permite en algunos casos la recopilación masiva de datos (incluido el contenido de las comunicaciones) mediante inteligencia de señales; si bien el Decreto nº 14086 contiene varias garantías en caso de recogida masiva, no prevé una autorización previa independiente para la recogida masiva; y ya, en la sentencia "Schrems II", el TJUE explicó que la vigilancia de los EE. UU. no cumplía el Derecho de la UE porque no exigía un "criterio objetivo" que permitiese justificar la injerencia del Gobierno en la privacidad.

81. Las garantías establecidas por los EE.UU. también facilitarán la circulación transatlántica de datos de forma más general, ya que también serán de aplicación a la transferencia de datos mediante otras herramientas como las cláusulas contractuales tipo[25] o las *Binding Corporate Rules*.

2. Rasgos característicos

82. Este nuevo Marco de Privacidad de Datos UE-EE.UU. responde a los siguientes 5 principios:

1º) **Transferencias legítimas y seguras:** con base en el nuevo marco de privacidad, los datos personales podrán transferirse de forma legítima y segura entre la UE y las compañías estadounidenses que se encuentren adheridas a dicho Marco.
2º) **Acceso a los datos estrictamente necesarios por parte de las Agencias de Inteligencia:** establecimiento de un nuevo conjunto de normas y garantías vinculantes con el fin de limitar el acceso a los datos por parte de las autoridades de inteligencia estadounidenses a lo necesario y respetando el principio de proporcionalidad para proteger la seguridad nacional. En este sentido, dichas agencias de inteligencia adoptarán procedimientos con el fin de garantizar una supervisión eficaz de los nuevos estándares de privacidad y libertades civiles.
3º) **Posibilidad de recurso para los titulares de los datos:** articulación de un nuevo procedimiento de recurso al alcance de los interesados en dos niveles, para investigar y resolver las reclamaciones de los titulares europeos sobre el acceso a sus datos por parte de las autoridades de inteligencia estadounidenses, que incluye el establecimiento de un Tribunal de revisión de protección de datos.
4º) **Necesidad de adhesión por las compañías estadounidenses:** fijación de obligaciones estrictas para las empresas estadounidenses que tratan datos personales transferidos desde la Unión Europea, incluyendo el requisito de "auto-certificar" su adhesión a los principios de este nuevo acuerdo.
5º) **Mecanismos de control y revisión:** se establecerán mecanismos específicos de control y revisión del marco de privacidad. La Comisión Europea, junto con representantes de las autoridades de protección de datos europeas y de las autoridades competentes estadounidenses, se ha comprometido a realizar una revisión periódica del funcionamiento del Marco de Privacidad de Datos UE-EE.UU. Y la primera revisión se llevará a cabo antes de que

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

se cumpla un año de la entrada en vigor de la decisión de adecuación (esto es, antes del 10 de julio de 2024), con objeto de verificar si todos los elementos pertinentes se han implantado plenamente y funcionan eficazmente en la práctica. Y el Departamento de Comercio estadounidense será el responsable de la administración y la supervisión del Marco. La Comisión Federal de Comercio de los EE.UU. se encargará de hacer cumplir por parte de las empresas estadounidenses.

83. El pasado 10 de julio de 2023, la Comisión Europea publicó su decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU. Se convierte en la tercera decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU.[26]

84. Los puntos clave de esta decisión son los siguientes:

a) Los servicios de inteligencia estadounidenses deberán limitar su acceso a los datos de la UE que sean necesarios y proporcionados a la protección de la seguridad nacional en el seno de una investigación realizada de acuerdo con la normativa de inteligencia exterior de los EEUU.
b) Los ciudadanos de la UE podrán acudir al nuevo *Data Protection Review Court* para impugnar las acciones y decisiones de las autoridades de inteligencia y para proteger sus derechos.
c) Si el *Data Protection Review Court* concluye que se han recogido datos incumpliendo las nuevas garantías, podrá requerir la supresión de los mismos.
d) Las nuevas garantías en materia de acceso a los datos por los servicios de inteligencia complementarán las obligaciones que las empresas estadounidenses que importen datos de la UE tendrán que asumir.
e) Las empresas estadounidenses podrán adherirse al Marco de Privacidad de Datos UE-EE. UU. si se comprometen a cumplir una serie de obligaciones detalladas de privacidad y obtienen la aprobación del *US Department of Commerce*, que se encargará de revisar y monitorizar si dichas empresas cumplen los requisitos.
f) Entre los requisitos a cumplir destaca la obligación de borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida;
g) También destaca la obligación de garantizar la continuidad de la protección si se comparten los datos de carácter personal con terceros.
h) En caso de tratamiento indebido de los datos por parte de las empresas estadounidenses, los ciudadanos de la UE dispondrán de varias vías de reparación entre las que destacan los mecanismos de resolución independiente y gratuita de controversias y un tribunal arbitral.
i) Serán también aplicables las cláusulas contractuales tipo y las normas corporativas vinculantes. Como consecuencia de estas nuevas garantías, los datos personales transferidos por las empresas europeas a empresas estadounidenses al amparo del nuevo marco no necesitarán de establecer garantías adicionales de protección de datos.[27]

85. Con la aprobación de este nuevo Acuerdo, la Comisión Europea espera, por un lado, dar carpetazo de una vez por todas, a la falta de garantías señalada por el TJUE y que provocó la invalidez de los dos marcos de privacidad anteriores (*Safe Harbor* y *Privacy Shield*); y, por otro lado, establecer un nuevo marco seguro y duradero, mediante el que se puedan realizar las transferencias de datos personales necesarias desde la UE a EE.UU.

[26] Decisión de ejecución de la Comisión de 10 de julio de 2023, de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo al nivel adecuado de protección de los datos personales en el marco de privacidad de datos entre UE y los EE.UU.

[27] *Vid.*, en sentido amplio, https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf.

86. Este es un acuerdo importante y necesario para facilitar el actual flujo de datos UE-EE. UU. y las relaciones comerciales con clientes, socios y proveedores de servicios en dicho país. No obstante, existen todavía muchas dudas en relación con este nuevo marco jurídico trasatlántico y si el mismo podrá realmente conseguir los objetivos que se propone. En especial, los retos que la legislación estadounidense relativa a vigilancia y espionaje (*FISA* y *EO 12333*) suponen para ofrecer unas garantías similares a las establecidas por la normativa de protección de datos personales vigente en la UE.

87. El nuevo marco introduce mejoras significativas en comparación con el mecanismo que existía bajo el Escudo de Privacidad. Por ejemplo, si el Tribunal de Revisión de Protección de Datos determina que los datos se recopilaron en violación de las nuevas salvaguardas, podrá ordenar la eliminación de los datos. Las nuevas salvaguardas en el ámbito del acceso gubernamental a los datos complementarán las obligaciones que tendrán que suscribir las empresas estadounidenses que importen datos de la UE.

88. Las empresas estadounidenses podrán unirse al nuevo Marco de Privacidad Unión Europea-EE.UU. comprometiéndose a cumplir con un conjunto detallado de obligaciones de privacidad, por ejemplo, el requisito de eliminar datos personales cuando ya no sean necesarios para el propósito para el que fueron recopilados, y garantizar la continuidad de la protección cuando los datos personales se comparten con terceros.

89. Las personas de la UE se beneficiarán de varias vías de reparación en caso de que las empresas estadounidenses manejen incorrectamente sus datos. Esto incluye mecanismos de resolución de disputas independientes y gratuitos y un panel de arbitraje.

90. La clave va a estar en la capacidad de las autoridades americanas de controlar posibles abusos en la gestión de datos, sobre todo por las instituciones de inteligencia de EEUU. Y los principales cambios de este nuevo acuerdo van en esa línea para dotar de seguridad jurídica este tipo de transferencias internacionales de datos. De esta forma se establecen procedimientos e instituciones para ese control de la actividad amparada por la normativa americana se alinee con los principios del RGPD, a nivel de proporcionalidad y minimización de los datos.

91. El funcionamiento de estas medidas va a radicar en la transparencia que existe en estos procesos de control. Es importante que el ciudadano tenga visibilidad sobre en qué se concretan esas medidas y si van a tener el efecto que se esperan. Sin lugar a dudas, las principales obligaciones son las de respetar los principios básicos que reconoce el Marco de Privacidad (muy similares a los que reconoce el RGPD). Sobre el proceso de certificación, para adherirse al Marco de Privacidad deberá demostrarse el cumplimiento con los anteriores principios tanto al momento de inscribirse por primera vez como con cada recertificación (obligatoriamente, las entidades deberán revalidar su certificación con carácter anual). Al mismo tiempo se reconocen modalidades de certificación vía (i) *self assessment* o (ii) por comprobación externa.[28]

92. Al examinar el nivel de protección ofrecido por un tercer país, la Comisión está obligada a evaluar el contenido de las normas aplicables en ese país derivadas de su legislación nacional o de sus compromisos internacionales, así como la práctica destinada a garantizar el cumplimiento de dichas normas; que, en caso de que dicha evaluación se considere insatisfactoria en términos de adecuación y equivalencia, la Comisión estará obligada a suspender la adecuación cuando deje de existir equivalencia.

93. Es evidente que la capacidad de transferir datos personales a través de las fronteras puede ser un motor fundamental de innovación, productividad y competitividad económica, siempre y cuando se ofrezcan unas garantías adecuadas; que estas transferencias deben realizarse con pleno respeto del

[28] *Vid.*, en sentido amplio, https://www.economistjurist.es/actualidad-juridica/eeuu-y-la-ue-llegan-a-un-nuevo-acuerdo-sobre-transferencias-internacionales-de-datos-que-blinda-la-privacidad-que-reclamaba-el-tjue/.

derecho a la protección de los datos personales y el derecho a la privacidad; y que uno de los fines de la UE es la protección de los derechos fundamentales consagrados en la Carta de derechos Fundamentales de la UE (en particular, el respeto de la vida privada y familiar y la protección de los datos personales).

94. Si bien el RGPD se aplica a todas las empresas que tratan datos personales de interesados en la UE cuando las actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la UE o con el seguimiento de su comportamiento en la medida en que este tenga lugar dentro de la UE, la recopilación indiscriminada de datos sin salvaguardias que limiten la intrusión en la privacidad de las personas por agentes estatales merma la confianza de los ciudadanos, las empresas y los Gobiernos europeos en los servicios digitales; y, por ende, en la economía digital; y, aunque a las agencias estadounidenses les está prohibida la recopilación masiva de datos sobre los ciudadanos estadounidenses que viven en ese país, dicha prohibición no se aplica en el caso de los ciudadanos de la UE; y esa vigilancia masiva por parte de agentes estatales es ilegal y afecta negativamente a la confianza de los ciudadanos y las empresas de la UE en los servicios digitales y, por ende, en la economía digital.

3. Especial atención a las reservas del Comité Europeo de Protección de Datos al nuevo Marco transatlántico de privacidad de datos

95. Hemos tenido que esperar casi 2 años desde la STJUE "Schrems II" para el restablecimiento del flujo de datos de carácter personal entre las empresas europeas y estadounidenses[29]. Tras la invalidación de la decisión de adecuación anterior sobre el Escudo de privacidad la UE-EE.UU. por parte del Tribunal de Justicia de la UE, la Comisión Europea y el Gobierno estadounidense se sentaron a negociar un nuevo marco que resolviera los problemas puestos de manifiesto por el propio TJUE.[30]

96. El pasado 25 de marzo de 2022 se publicó una Declaración conjunta de la Comisión Europea y los EE.UU. sobre el marco transatlántico de privacidad de datos. Dicha Declaración constituye un nuevo Marco Trasatlántico de Privacidad de Datos, que pretende fomentar los flujos de datos transatlánticos y abordará las preocupaciones planteadas por "Schrems II". El nuevo Marco fijaba un compromiso sin precedentes por parte de EE.UU. para implementar reformas que fortalecerán las protecciones de privacidad y libertades civiles aplicables a las actividades de inteligencia de señales de EE.UU. Bajo el Marco Transatlántico de Privacidad de Datos, EE.UU. implementará nuevas salvaguardas para garantizar que las actividades de vigilancia de señales sean necesarias y proporcionadas en la búsqueda de objetivos definidos de seguridad nacional, establecerá un mecanismo de reparación independiente de dos niveles con autoridad vinculante para medidas correctivas directas y mejorar la supervisión rigurosa y en capas de las actividades de inteligencia de señales para garantizar el cumplimiento de las limitaciones en las actividades de vigilancia.

97. Se señalaba, entonces, que sería el Comité Europeo de Protección de datos (CEPD) quien debía analizar el documento antes de que se adoptase una decisión en firme, tal y como recoge el RGPD. El CEPD recordó que, de momento, el anuncio no constituía un marco legal, por lo que los exportadores de datos **tendrían/tienen que seguir cumpliendo con las medidas impuestas** por el TJUE y a partir de la sentencia "Schrems II". Y, así las cosas, el CEPD, en su reunión plenaria del pasado 28 de febrero de 2023, emitió un dictamen sobre el Proyecto de Decisión de Adecuación, publicado por la Comisión Europea el 13 de diciembre de 2022, sobre el nuevo Marco para los intercambios transatlánticos de datos personales entre la UE y los EE.UU.[31]

[29] *Vid.* A. Ortega giménez/ e. García escobar, "Comentario a la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2020 ("Schrems II")", en *LA LEY Privacidad*, número 6, Editorial Wolters Kluwer, Madrid, octubre-diciembre 2020, pp. 1-22.

[30] *Vid.*, en sentido amplio, https://www.tendencias.kpmg.es/2022/03/claves-acuerdo-principios-ue-ee-uu-marco-transatlantico-privacidad-datos.

[31] *Vid.* https://diariolaley.laleynext.es/dll/2023/03/06/el-comite-europeo-de-proteccion-de-datos-emite-un-dictamen-favorable-con-reservas-al-nuevo-marco-de-transferencia-de-datos-a-los-estados-unidos.

98. El Dictamen del CEPD[32] reconoce los aspectos positivos incorporados tras la negociación, al tiempo que señala determinadas deficiencias que no han sido resueltas, representando riesgos desde la óptica de la protección de datos personales. Dichas deficiencias afectan tanto a la parte comercial de dicho marco, es decir, a las transferencias de datos desde las empresas en Europa a las empresas en EE.UU., como al acceso que desde las autoridades de seguridad gubernamentales de EEUU se prevé a los datos personales que se transfieran a EE.UU. El CEPD ha presentado su dictamen al Parlamento Europeo, dando así continuidad al proceso de tramitación de dicho Acuerdo en la UE hasta su posible aprobación definitiva.

99. En su Dictamen 5/2023, el CEPD acoge con satisfacción mejoras sustanciales introducidas en relación con el marco anterior regulado por el Acuerdo *Privacy Shield*, tales como la introducción de los principios de necesidad y proporcionalidad para la recogida de datos por los servicios de inteligencia de EE.UU. y el nuevo mecanismo de recurso para los interesados de la UE; pero, al mismo tiempo, expresa su preocupación y solicita aclaraciones sobre varios puntos incluidos en la nueva propuesta.

100. Se señala que el marco de privacidad propuesto es una mejora respecto el anterior, pero no suficiente como para justificar una decisión de adecuación sobre las transferencias de datos personales, por lo que se oponen a éste.

101. Argumentan que la Comisión Europea no debería otorgar a los EE.UU. una decisión de adecuación que considere que su nivel de protección de datos personales sea esencialmente equivalente al de la UE y permita la transferencia de datos personales entre la UE y EE. UU. Recalcando que se continúa permitiendo la recopilación masiva de datos y que, a pesar de la creación de un Tribunal de Revisión de Protección de Datos, destinado a proporcionar a los interesados de la UE reparación en caso de vulneración de derechos**,** se trata de un tribunal que lleva a cabo decisiones secretas y que vulnera el derecho de los ciudadanos a acceder y rectificar los datos sobre ellos**,** además, de no tener plena independencia.

102. Concluyen indicando que se presenta un marco de privacidad que no se encuentra preparado para el futuro y que la evaluación de la adecuación debe basarse en la aplicación práctica de las normas. Por esto, entienden que la Comisión Europea no debería otorgar una decisión de adecuación basada en el régimen actual, sino que debería negociar nuevamente un nuevo acuerdo que mejore los puntos expuestos.

103. Y mientras todo esto ocurre, un nuevo terremoto en material de transferencias internacionales de datos de carácter personal se ha producido: hemos tenido conocimiento de la multa récord de 1200 millones de euros impuesta a Meta por parte del regulador irlandés por violar las normas europeas de protección de datos con su red social Facebook.

104. Meta, que pretende apelar, es condenada por haber continuado transfiriendo datos personales de usuarios de la UE a los EE.UU. violando las normas europeas en la materia, indicó en su decisión la Comisión Irlandesa de Protección de Datos. (DPC), que actúa en nombre de la UE.

105. Meta también debe suspender cualquier transferencia de datos personales a los EE.UU. en los próximos cinco meses tras la notificación de esta decisión y debe cumplir con la protección de datos en los próximos seis meses. Esta sanción, la más alta impuesta por un regulador de protección de datos en la UE, es el resultado de una investigación iniciada en 2020, y tiene su fundamentación jurídica en la vulneración del artículo 46 del RGPD, que señala que "el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas".

[32] Puede accederse al contenido completo del Dictamen 5/2023 a través del enlace: https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf.

106. Esta es la tercera multa impuesta a Meta desde principios de año en la UE y la cuarta en seis meses. En enero, la Comisión Irlandesa de Protección de Datos. (DPC) había sancionado duramente al grupo con casi 400 millones de euros por delitos sobre el uso de datos personales con fines publicitarios dirigidos a sus aplicaciones de Facebook, Instagram y WhatsApp, luego, en marzo, con 5,5 millones de euros por violar la protección de datos con su mensaje de WhatsApp. Desde entonces, Meta se comprometió a cambiar sus términos de uso en Europa para poder continuar recopilando y procesando los datos personales de sus usuarios europeos. Estas sanciones se dan en un contexto de refuerzo de los controles y procedimientos judiciales en la UE, pero también en EE.UU., contra GAFA (Google, Amazon, Facebook y Apple), y las medidas tomadas recientemente contra el gigante chino TikTok. En 2021, Amazon recibió una multa de 746 millones de euros en Luxemburgo por incumplimiento de la normativa de protección de datos.

4. Valoración crítica

107. Al examinar el nivel de protección ofrecido por un tercer país, la Comisión está obligada a evaluar el contenido de las normas aplicables en ese país derivadas de su legislación nacional o de sus compromisos internacionales, así como la práctica destinada a garantizar el cumplimiento de dichas normas; que, en caso de que dicha evaluación se considere insatisfactoria en términos de adecuación y equivalencia, la Comisión debe abstenerse de adoptar una decisión de adecuación, ya que está supeditada a la aplicación de las garantías pertinentes; que la Comisión está obligada a suspender la adecuación cuando deje de existir equivalencia; que el RGPD exige que la evaluación pertinente sea un proceso continuo que tenga en cuenta los cambios en las normas y prácticas aplicables.

108. Sin ninguna duda la capacidad de transferir datos personales a través de las fronteras puede ser un motor fundamental de innovación, productividad y competitividad económica, siempre y cuando se ofrezcan unas garantías adecuadas; que estas transferencias deben realizarse con pleno respeto del derecho a la protección de los datos personales y el derecho a la privacidad; y que uno de los fines de la UE es la protección de los derechos fundamentales consagrados en la Carta (en particular, el respeto de la vida privada y familiar y la protección de los datos personales).

109. Si bien el RGPD se aplica a todas las empresas que tratan datos personales de interesados en la Unión cuando las actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión o con el seguimiento de su comportamiento en la medida en que este tenga lugar dentro de la UE, la recopilación indiscriminada de datos sin salvaguardias que limiten la intrusión en la privacidad de las personas por agentes estatales merma la confianza de los ciudadanos, las empresas y los Gobiernos europeos en los servicios digitales y, por ende, en la economía digital; y, aunque a las agencias estadounidenses les está prohibida la recopilación masiva de datos sobre los ciudadanos estadounidenses que viven en ese país, dicha prohibición no se aplica en el caso de los ciudadanos de la UE; y esa vigilancia masiva por parte de agentes estatales es ilegal y afecta negativamente a la confianza de los ciudadanos y las empresas de la UE en los servicios digitales y, por ende, en la economía digital.

110. A pesar de que no existe legislación federal en materia de privacidad y protección de datos en los EE.UU., son notables los esfuerzos realizados por los EE.UU. en el Decreto n.º 14086, introduce definiciones de conceptos fundamentales de la protección de datos, como los principios de necesidad y proporcionalidad, y supone un importante paso adelante con respecto a mecanismos de transferencia anteriores, para fijar límites a las actividades de inteligencia de señales de los EE.UU. haciendo que los principios de proporcionalidad y necesidad sean aplicables al marco jurídico estadounidense en materia de inteligencia de señales e incorporando una lista de objetivos legítimos para dichas actividades.

111. Si bien el citado Decreto prevé importantes mejoras destinadas a garantizar que estos principios sean sustancialmente equivalentes a los contemplados en el Derecho de la UE, estos principios

son desde hace tiempo elementos clave del régimen de protección de datos de la UE y sus definiciones sustantivas recogidas en el Decreto n. º 14086 no están en consonancia con su definición en el Derecho de la UE y su interpretación por parte del TJUE.

112. En la medida en que el Decreto n. º 14086 permite en algunos casos la recopilación masiva de datos (incluido el contenido de las comunicaciones) mediante inteligencia de señales; si bien el Decreto n. º 14086 contiene varias garantías en caso de recogida masiva, no prevé una autorización previa independiente para la recogida masiva; y ya en la sentencia "Schrems II", el TJUE explicó que la vigilancia de los EE. UU. no cumplía el Derecho de la UE porque no exigía un "criterio objetivo" que permitiese justificar la injerencia del Gobierno en la privacidad.

113. Se deben compartir las preocupaciones del CEPD en la medida en que el Decreto n.º 14086 no proporcione garantías suficientes respecto a la recopilación masiva de datos al no prever una autorización previa independiente, carecer de normas claras y estrictas sobre la conservación de los datos, permitir una recopilación masiva «temporal» y no establecer exigencias más estrictas en relación con la difusión de los datos recopilados de forma masiva; señala, en particular, la preocupación específica de que, si no se aplican restricciones adicionales a la transmisión a las autoridades estadounidenses, los servicios de seguridad podrían acceder a datos a los que, de otro modo, se les habría prohibido acceder; recuerda que las transferencias ulteriores multiplican de hecho los riesgos para la protección de datos.

114. El Decreto n.º 14086 introduce algunas garantías para velar por la independencia de los jueces del TRPD, como también reconoce el CEPD; el TRPD forma parte del poder ejecutivo y no del poder judicial y que sus jueces son nombrados para un mandato fijo de cuatro años; el presidente de los EE.UU. puede revocar las decisiones del TRPD e incluso hacerlo en secreto; señala que, aunque el nuevo mecanismo de recurso no permite al fiscal general de los EE.UU. destituir y supervisar a los jueces del TRPD, no afecta a las facultades correspondientes del presidente de los EE.UU.; subraya que, mientras el presidente de los EE.UU. pueda destituir a los jueces del TRPD durante su mandato, la independencia de estos no estará garantizada; en caso de adopción, la Comisión debería seguir de cerca la aplicación de salvaguardas que garanticen la independencia en la práctica; señala que los demandantes estarían representados por un "abogado especial" designado por el TRPD y no sujeto a requisitos de independencia; pide a la Comisión que, en caso de que se adopte una decisión de adecuación, vele por que se introduzca un requisito de independencia; concluye que, a día de hoy, el TRPD no cumple las normas de independencia e imparcialidad establecidas en el artículo 47 de la Carta; y, si bien la Junta de supervisión de la intimidad y las libertades civiles examinaría de forma independiente el funcionamiento del nuevo proceso de recurso, el alcance de este examen sería limitado;

115. Si bien los EE.UU. han previsto un nuevo mecanismo de recurso para las cuestiones relacionadas con el acceso de las autoridades públicas a los datos, siguen existiendo dudas sobre la efectividad de las vías de recurso disponibles en materia comercial, respecto a las cuales la decisión de adecuación no introduce cambios; observa que los mecanismos para resolver estas cuestiones se dejan en gran medida a la discreción de las empresas, que pueden elegir vías alternativas de solución, como los mecanismos de resolución de litigios o el uso de los programas de privacidad de las empresas; pide a la Comisión que, en caso de que se adopte una decisión de adecuación, supervise de cerca la eficacia de estos mecanismos de recurso;

116. A diferencia de todos los demás terceros países que han recibido una decisión de adecuación en virtud del RGPD, los EE.UU. no cuentan con una ley federal de protección de datos. La aplicación del Decreto n. º 14086 no es clara, precisa ni previsible, ya que puede ser modificado en cualquier momento por el presidente de los EE. UU., quien también está facultado para emitir decretos secretos; observa que la revisión de la decisión de adecuación tendría lugar transcurrido un año a partir de la fecha de notificación de la decisión de adecuación a los Estados miembros y, posteriormente, al menos cada cuatro años.

117. Las preocupaciones expresadas por el CEPD en relación con los derechos de los interesados, la ausencia de definiciones fundamentales y de normas específicas sobre la toma de decisiones automatizada y sobre la elaboración de perfiles, la falta de claridad sobre la aplicación de los principios del marco de privacidad a los encargados del tratamiento y la necesidad de evitar que las transferencias ulteriores socaven el nivel de protección son compartidas.

118. Las decisiones de adecuación, que deben ser adoptadas sobre la base de la legislación y las prácticas vigentes, no solo en cuanto al fondo, sino también en la práctica, tal como se establece en la STJUE "Schrems I", en la STJUE "Schrems II" y en el propio RGPD (Considerando 104), deben incluir mecanismos claros y estrictos de seguimiento y revisión a fin de garantizar que las decisiones estén preparadas para el futuro o que puedan revocarse o modificarse según proceda, y que se garantice en todo momento el derecho fundamental de los ciudadanos de la UE a la protección de datos y el Marco Transatlántico de Privacidad de Datos debería estar sujeto a una revisión permanente en función de la evolución jurídica y práctica en los EE.UU. [33]

5. Perspectivas de futuro

119. Así las cosas, ¿podríamos decir que "a la tercera va la vencida?...pues la verdad es que no lo tenemos muy claro. A la misma vez que se anunciaba la puesta de largo del nuevo Marco de Privacidad de Datos UE-EE.UU. Edward Snowden se pronunciaba: este nuevo marco jurídico es en gran medida una copia del "Escudo de Privacidad". El tercer intento de la Comisión Europea de conseguir un acuerdo estable sobre las transferencias de datos entre la UE y EE.UU. volverá probablemente al TJUE en cuestión de meses. El "nuevo" Marco Transatlántico de Privacidad de Datos es en gran medida una copia del fracasado "Escudo de Privacidad". A pesar de los esfuerzos de relaciones públicas de la Comisión Europea, hay pocos cambios en la legislación estadounidense o en el enfoque adoptado por la UE. EE.UU. no se abordó el problema fundamental de la ley FISA 702, ya que sigue considerando que sólo las personas estadounidenses son merecedoras de derechos constitucionales.[34]

120. En 2013 Edward Snowden reveló que el Gobierno de EE.UU. utilizaba empresas de "grandes tecnologías" y programas como "PRISM" o "Upstream" al amparo de la FISA 702 y la OE 12.333 para espiar al resto del mundo sin necesidad de causa probable ni aprobación judicial. Esto no se limitaba a la delincuencia o el terrorismo, sino que también incluía el espionaje a "socios" de EE.UU. Desde una ley de la UE de 1995, en general no se pueden enviar datos personales fuera de la UE a menos que exista una protección "esencialmente equivalente" en el país de destino. La industria estadounidense se basó en gran medida en una Decisión de la Comisión Europea llamada "Safe Harbor" (Puerto Seguro) que declaró a EE.UU. "esencialmente equivalente" en 2000. El TJUE anuló la Decisión de la Comisión en el asunto C-362/14 ("Schrems I") en 2015, dadas las leyes de vigilancia de EEUU. En 2016, la Comisión Europea ha aprobado en gran medida la misma Decisión sobre transferencias de datos UE-EE.UU. de nuevo, bajo el nuevo nombre de «Escudo de Privacidad», que fue invalidado por el TJUE en C-311/18 ("Schrems II") en 2020 en gran medida por los mismos motivos.

121. Tras la anulación del "Escudo de la privacidad", las negociaciones entre la UE y EE.UU. apenas avanzaron. EE.UU. insistió en que los datos de la UE seguirían sujetos a la vigilancia masiva estadounidense y que las personas "no estadounidenses" *no* tendrían las mismas protecciones que las estadounidenses. Tras más de año y medio sin apenas movimiento, EE.UU. habría utilizado la guerra de Ucrania para presionar a la UE sobre el intercambio de datos personales. Poco después, Joe Biden y Ursula von der Leyen se reunieron el 25 de marzo de 2022. Ese mismo día, los dos han "resuelto"

[33] *Vid.* Resolución del Parlamento Europeo, de 11 de mayo de 2023, sobre la adecuación de la protección conferida por el marco de privacidad de datos UE-EE. UU. (2023/2501(RSP)).

[34] *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

de repente lo que los abogados eran incapaces de resolver y han presentado un"acuerdo de principio", un pagaré que en esencia contenía dos "trucos" que deberían calmar a la opinión pública: a) e*n primer lugar*, el TJUE consideró que **la vigilancia masiva FISA 702 no era «proporcionada»** en el sentido del artículo 52 de la Carta de los Derechos Fundamentales de la UE (CFR). La «nueva» Orden Ejecutiva 14086 de EE.UU. (que equivale en gran medida a la PPD-28 de 2014) incluiría ahora la palabra "proporcionada". El "truco" aquí: EEUU atribuirá otro significado a la palabra "proporcionado" que el TJUE. La OE 14086 declara que la vigilancia masiva FISA 702 es "proporcionada" en virtud de una "interpretación estadounidense" no revelada de la palabra y contraria a las dos conclusiones del TJUE. De este modo, la UE y EE.UU. pudieron afirmar que estaban de acuerdo en la misma palabra ("proporcionada"), incluso cuando no hay acuerdo sobre el significado de la palabra; y, *b) en segundo lugar*, el TJUE determinó que la compensación a través del "Defensor del Pueblo" del Escudo de Privacidad no cumplía ni remotamente con el artículo 47 del MCR , incluso cuando el Defensor del Pueblo fue aclamado por las relaciones públicas de la Comisión en 2016 como una forma "*independiente"* de «*compensación en el ámbito de la seguridad nacional*". El "truco" de la reparación: el mecanismo del Defensor del Pueblo fue **renombrado y dividido en un Oficial de Protección de las Libertades Civiles (CLPO) y un llamado «Tribunal** « (que no es un tribunal, sino un órgano ejecutivo parcialmente independiente). Aunque hay algunas mejoras menores con respecto al Defensor del Pueblo, el individuo no tendrá ninguna interacción directa con los nuevos organismos (tendrá que enviar una queja a una autoridad de protección de datos de la UE y no será escuchado por EE.UU.) y darán exactamente la misma respuesta que el anterior «Defensor del Pueblo». Según la OE 14086, el CLPO y el Tribunal deberán responder en cualquier caso diciendo: *"Sin confirmar ni negar que el denunciante estuviera sometido a actividades de inteligencia de señales de EE.UU., la revisión o bien no identificó ninguna violación cubierta o bien el Tribunal de Revisión de Protección de Datos emitió una resolución que exigía una reparación adecuada*" (ver aquí). Por lo tanto, la "sentencia" de este "Tribunal" se conoce incluso antes de que se presente un caso. Hay muchos problemas adicionales con el mecanismo, que garantizarán en gran medida que las denuncias ni siquiera sean admitidas. Parece impensable que el Tribunal de Justicia acepte esto como "recurso judicial" en virtud del artículo 47 del MCR.

122. EE.UU. se ha negado a reformar la FISA 702 para ofrecer a las personas no estadounidenses una protección razonable de la intimidad. Hay acuerdo a ambos lados del Atlántico en que la FISA 702 y la OE 12.333 violan derechos fundamentales en virtud de la 4ª Enmienda en EE.UU. y de los artículos 7, 8 y 47 del CFR en la UE, pero EE.UU. sigue insistiendo en que las personas no estadounidenses no tienen derechos constitucionales en EE.UU., por lo que una violación de su derecho a la intimidad no está cubierta por la 4ª Enmienda. FISA 702 tendrá que prorrogarse a finales de 2023, dado que existe una "cláusula de extinción" en la legislación estadounidense. Esta habría sido la oportunidad perfecta para mejorar la ley estadounidense, pero dado el nuevo acuerdo con la UE, habrá pocas razones para que EE.UU. reforme la FISA 702[35].

123. En general, el nuevo "Marco Transatlántico de Privacidad de Datos" es una copia de *Privacy Shield* (de 2016), que a su vez era una copia de *Safe Harbour* (de 2000). Dado que este enfoque ya ha fracasado dos veces, no había base jurídica para el cambio de rumbo: la única lógica de llegar a un acuerdo era política.

[35] Señala Max Schrems, presidente de *Noyb*: "dicen que la definición de locura es hacer lo mismo una y otra vez y esperar un resultado diferente. Al igual que el "Escudo de la privacidad", el último acuerdo no se basa en cambios materiales, sino en intereses políticos. Una vez más, la actual Comisión parece pensar que el lío será problema de la próxima Comisión. La FISA 702 debe ser prorrogada por EE.UU. este año, pero con el anuncio del nuevo acuerdo la UE ha perdido todo poder para conseguir una reforma de la FISA 702". Es más, "ahora tenemos 'Puertos', 'Paraguas', 'Escudos' y 'Marcos', pero ningún cambio sustancial en la legislación estadounidense sobre vigilancia. Las declaraciones de prensa de hoy son casi una copia literal de las de hace 23 años. El mero anuncio de que algo es "nuevo", "sólido" o "eficaz" no basta ante el Tribunal de Justicia. Necesitaríamos cambios en la legislación estadounidense sobre vigilancia para que esto funcionara, y sencillamente no los tenemos." *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

124. Cualquier persona cuyos datos personales vayan a ser transferidos en virtud del nuevo acuerdo puede presentar un recurso ante las autoridades de protección de datos o los tribunales. *noyb* ha preparado varias opciones procesales para llevar el nuevo acuerdo ante el TJUE. Esperamos que el nuevo sistema sea aplicado por las primeras empresas en los próximos meses, lo que abrirá la vía a la impugnación por parte de una persona cuyos datos se transfieran en virtud del nuevo instrumento. No es improbable que una impugnación llegue al TJUE a finales de 2023 o principios de 2024. El TJUE tendría entonces incluso la opción de suspender el "Marco" durante el tiempo que dure el procedimiento. Una decisión final del TJUE sería probable para 2024 o 2025. Independientemente de que la impugnación prospere, esto aportará claridad al "Marco Transatlántico de Privacidad de Datos" dentro de unos dos años.[36]

125. Este tercer intento de aprobar en gran medida la misma decisión ilegal también plantea interrogantes sobre el papel más amplio de la Comisión Europea como guardiana de los tratados de la UE. En lugar de defender el "Estado de derecho", la Comisión se limita a aprobar una decisión inválida una y otra vez, a pesar de las claras sentencias del TJUE. A pesar de la gran indignación tras las revelaciones de Snowden en la UE y de los repetidos llamamientos del Parlamento Europeo a tomar medidas, la Comisión parece dar prioridad a las relaciones diplomáticas con EE.UU. y a la presión empresarial a ambos lados del Atlántico sobre los derechos de los europeos y los requisitos de la legislación de la UE[37].

VI. Conclusiones

126. PRIMERA. - El imparable (y peligroso) aumento de las transferencias internacionales de datos de carácter personal. El acceso y uso de la información por parte de empresas, administraciones e individuos se ha convertido en un precioso bien intangible, causa y efecto a la vez de la progresiva integración económica y social. Junto a la dimensión económica, la protección de los datos personales y de la intimidad supone afrontar por vez primera la difícil tarea de compatibilizar los derechos fundamentales con el comercio internacional; y todo ello en cada una de las distintas esferas jurídicas implicadas. La búsqueda de una solución que ampare ambos intereses en las transferencias internacionales de datos en un contexto global no es fácil, debido sobre todo, a las diferencias entre los distintos niveles de protección de los derechos y libertades de las personas y su intimidad existentes entre distintos estados. En este sentido, la búsqueda de soluciones uniformes ha de superar las distintas calificaciones en las categorías de datos personales y los distintos intereses económicos en juego, dada la original vinculación de los datos con el desarrollo del comercio internacional. Las acciones concertadas permitirían, además de un aumento de la eficacia y la seguridad jurídicas, la consecución de economías sobre los costes de circulación internacional de la información, impidiendo la constitución de los comentados "paraísos de datos" y la deslocalización de actividades informáticas.

127. La especial volatilidad de las transferencias internacionales de datos complica extraordinariamente la definición del derecho sustantivo aplicable. Las características de los flujos de información y el carácter abierto de las redes posibilitan el acceso a los datos, así como su recopilación y tratamientos desde varios países de manera simultánea, por lo que distintos estados tendrán competencia normativa para definir los términos y las condiciones de las prácticas apropiadas en el ámbito de la información.

[36] Max Schrems: *«Tenemos varias opciones de impugnación ya en el cajón, aunque estamos hartos de este ping-pong jurídico. Actualmente esperamos que esto vuelva al Tribunal de Justicia a principios del año que viene. El Tribunal de Justicia podría incluso suspender el nuevo acuerdo mientras revisa su contenido. En aras de la seguridad jurídica y el Estado de Derecho, entonces sabremos si las pequeñas mejoras de la Comisión han sido suficientes o no.* Durante los *últimos 23 años, todos los acuerdos entre la UE y EE.UU. han sido declarados inválidos con carácter retroactivo, haciendo ilegales todas las transferencias de datos realizadas por las empresas en el pasado; parece que ahora vamos a añadir otros dos años de este ping-pong*". *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

[37] Max Schrems: "se supone que la Comisión es la 'guardiana de los tratados' y la defensora del 'Estado de Derecho'. Le encanta ese papel cuando se trata de que los Estados miembros violen la legislación de la UE. Ahora la propia Comisión simplemente ignora al Tribunal de Justicia por tercera vez". *Vid.* https://noyb.eu/es/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

128. SEGUNDA. - Diferente enfoque acerca de la protección del derecho fundamental a la protección de datos de carácter personal entre la UE y los EE.UU. en tres actos. El fracaso de los *Safe Harbour* tuvo una razón de ser clara: ya que a los ojos de la Directiva, era posible que las exportaciones de datos de carácter personal a los EE.UU. fueran prohibidas ya que mientras el enfoque de EEUU en esta materia se basaba en una mezcla de legislación, reglamentación y autorregulación, la UE consideraba imprescindible la protección del derecho fundamental a la privacidad.

Gráficamente podemos reseñar ese diferente enfoque en dos actos:

Acto Primero: STJUE "Schrems I"

129. Varios fueron los interrogantes (sin respuesta) que las condiciones de aplicación e imposición del Acuerdo UE-EE.UU. nos planteó: ¿Qué repercusión tendrá en la función de las autoridades nacionales de control la elección de una sociedad estadounidense con quejas incursas ante un organismo específico?; en el ámbito europeo, cuando se tramiten las quejas, ¿cuáles serán las competencias respectivas de las autoridades nacionales de control y de la UE?; en el caso de procedimientos que tengan lugar en EE.UU. y en la UE de manera simultánea o sucesiva y que resulten en posturas contrarias respecto de una misma queja, ¿cómo se resolverán las diferencias?

130. Y, sobre el contenido de los Principios de *Safe Harbour*, se debió poner la atención, en particular, en alguno de ellos: por un lado, hubiera sido aconsejable reforzar el Principio de "Opción", ya que los principios de puerto seguro no regulaban la legitimidad de los criterios de tratamiento; y, por otro lado, respecto del principio de "Acceso", pensamos que las excepciones que contenían las FAQ eran demasiado generales, era preciso abarcar los datos públicos; y, c) que los datos cuyo tratamiento vulnerase los principios habrían de corregirse o suprimirse. Quizás estos interrogantes precipitaron el resultado de sobra conocido por todos: el TJUE declaró inválida la Decisión 2000/520/CE que consideraba que los principios de Puerto Seguro garantizaban un nivel adecuado de protección de los datos transferidos desde la UE a empresas norteamericanas (STJUE "Scherems I")-

Acto Segundo: STJUE "Schrems II"

131. La STJUE "Schrems II" resolvió un total de once cuestiones prejudiciales planteadas por la High Court (Tribunal Superior, Irlanda), que el TJUE agrupó, para su resolución, en cinco cuestiones que se referían a la aplicabilidad del RGPD a las transferencia de datos a terceros países extracomunitarios, cuando en dichos países los datos pueden ser tratados por las autoridades con fines de seguridad nacional, defensa y seguridad del Estado; a los elementos integrantes del nivel de protección adecuado en terceros países; a las competencias y facultades de las autoridades de control en dichas transferencias; así como a la validez tanto de la Decisión 2010/87/UE relativa a las cláusulas contractuales tipo bajo el prisma de la Carta de Derechos Fundamentales de la UE, como de la Decisión "Escudo de Privacidad", así como el grado de garantía de la tutela judicial efectiva que, para los ciudadanos de la Unión Europea, ofrece la figura del Defensor del Pueblo mencionado en esta última Decisión.

132. El TJUE interpretó el nivel de protección adecuado para la transferencia de datos a terceros países en el sentido de que las garantías adecuadas, los derechos exigibles y las acciones legales efectivas requeridas las disposiciones normativas de los terceros países deben garantizar que los derechos de las personas cuyos datos personales se transfieren a dicho país, sobre la base de cláusulas tipo de protección de datos, gozan de un nivel de protección, sustancialmente, equivalente al garantizado dentro de la Unión Europea por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea.

133. En cuanto a las facultades de las autoridades de control competentes en el caso de transferencias de datos protegidos a terceros países extracomunitarios, diferencia el TJUE entre si existe o no

de una decisión de adecuación dictada por la Comisión. En el caso de que exista una decisión de adecuación, y mientras que la misma no haya sido objeto de invalidación por el TJUE, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, aunque tienen la potestad de interponer recurso ante los tribunales nacionales para que éstos formulen una cuestión prejudicial, ante el TJUE, sobre la validez de la decisión de adecuación. Por el contrario, en el caso de que no exista una decisión de adecuación emitida por la Comisión, el Tribunal resuelve que la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión, cuando esa autoridad de control considera, que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero.

134. El TJUE, en la Sentencia "Schrems II", declaró la validez de la Decisión 2010/87/UE por cuanto que ésta prevé mecanismos efectivos que permiten en la práctica garantizar que la transferencia a un país tercero de datos personales sobre la base de las cláusulas tipo de protección de datos recogidas en el anexo de la antedicha Decisión se prohíba o suspenda cuando el destinatario de la transferencia no cumpla las referidas cláusulas o no le resulte posible cumplirlas, incluyendo la posibilidad de control por las autoridades en el caso de que por el responsable del tratamiento no se suspenda o prohíba la transferencia.

135. En consecuencia, el TJUE declaró la invalidez de la Decisión "Escudo de Privacidad" teniendo en cuenta, por una parte, que las injerencias resultantes de los programas de vigilancia basados en la normativa de los EE.UU. no ofrecen un nivel de protección, sustancialmente, equivalente al garantizado dentro de la Unión Europea por el RGPD, interpretado a la luz de la Carta de los Derechos Fundamentales de la Unión Europea y, por otra parte, que el mecanismo del Defensor del Pueblo previsto en la Decisión "Escudo de Privacidad", no subsana las limitaciones al derecho a la tutela judicial efectiva, poniendo en entredicho la independencia del Defensor del Pueblo con respecto al poder ejecutivo de los EE.UU., poniendo de manifiesto, además, que no existe ninguna garantía legal que pueda ser invocada por los ciudadanos ante dicho Defensor del Pueblo, por lo que no se cumple con la exigencia de una vía de recurso efectivo garante del derecho a la tutela judicial efectiva en materia de protección de datos.

136. TERCERA. - Hacia la restauración de la confianza y la estabilidad en los flujos de datos trasatlánticos. Las transferencias internacionales de datos de carácter personal UE-EE.UU. siguen al orden del día con el nuevo Acuerdo UE-EE.UU. flujos de datos transatlánticos.

137. El pasado 10 de julio de 2023 la Comisión Europea publicó su decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU. Se convierte en la tercera decisión de adecuación relativa al Marco de Privacidad de Datos UE-EE.UU. Los puntos clave de esta decisión son los siguientes: a) Los servicios de inteligencia estadounidenses deberán limitar su acceso a los datos de la UE que sean necesarios y proporcionados a la protección de la seguridad nacional en el seno de una investigación realizada de acuerdo con la normativa de inteligencia exterior de los EEUU.; b) Los ciudadanos de la UE podrán acudir al nuevo Data Protection Review Court para impugnar las acciones y decisiones de las autoridades de inteligencia y para proteger sus derecho; c) Si el Data Protection Review Court concluye que se han recogido datos incumpliendo las nuevas garantías, podrá requerir la supresión de los mismos; d) Las nuevas garantías en materia de acceso a los datos por los servicios de inteligencia complementarán las obligaciones que las empresas estadounidenses que importen datos de la UE tendrán que asumir; e) Las empresas estadounidenses podrán adherirse al Marco de Privacidad de Datos UE-EE.UU. si se comprometen a cumplir una serie de obligaciones detalladas de privacidad y obtienen la aprobación del US Department of Commerce, que se encargará de revisar y monitorizar si dichas empresas cumplen los requisitos; f) Entre los requisitos a cumplir destaca la obligación de borrar los datos personales cuando ya no sean necesarios para el fin que hubiera motivado su recogida; g) También destaca la obligación de garantizar la continuidad de la protección si se comparten los datos de carácter personal con terceros; h) En caso de tratamiento indebido de los datos por parte de las empresas estadounidenses, los ciudadanos de la UE dispondrán de varias vías de reparación entre las que destacan los mecanismos de resolución

independiente y gratuita de controversias y un tribunal arbitral; y, finalmente, i) Serán también aplicables las cláusulas contractuales tipo y las normas corporativas vinculantes. Como consecuencia de estas nuevas garantías, los datos personales transferidos por las empresas europeas a empresas estadounidenses al amparo del nuevo marco no necesitarán de establecer garantías adicionales de protección de datos.[38]

138. En definitiva, este nuevo Marco de Privacidad de Datos UE-EE.UU. no da lugar a una equivalencia sustancial en el nivel de protección; se debería crear un mecanismo que garantice dicha equivalencia y que proporcionase el nivel adecuado de protección exigido por la legislación de la UE en materia de protección de datos y la Carta de Derechos Fundamentales de la UE, según la interpretación del TJUE y todas las recomendaciones formuladas, en su día, por el Parlamento Europeo y por el CEPD. Así las cosas, en un horizonte no muy lejano, se vislumbra un "Schrems III"… ¡Ojalá nos equivoquemos!

[38] *Vid.*https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework.pdf.