COMISIÓN
EUROPEA

Bruselas, 6.11.2015
COM(2015) 566 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE de forma consiguiente a la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems)

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE de forma consiguiente a la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems)

1. INTRODUCCIÓN: LA ANULACIÓN DE LA DECISIÓN SOBRE PUERTO SEGURO

La sentencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo «el Tribunal de Justicia» o «el Tribunal») de 6 de octubre de 2015 en el asunto C-362/14 (Schrems)[1] reafirma la importancia del derecho fundamental a la protección de los datos personales consagrado en la Carta de los Derechos Fundamentales de la UE, incluso cuando esos datos son transferidos fuera de la UE.

Las transferencias de datos personales constituyen un elemento esencial de la relación transatlántica. La UE es el principal socio comercial de los Estados Unidos, y viceversa, y las transferencias de datos forman, cada vez en mayor medida, parte integrante de sus intercambios comerciales.

Para facilitar esos flujos de datos, asegurando al mismo tiempo un alto nivel de protección de los datos personales, la Comisión reconoció la adecuación del régimen de puerto seguro mediante la adopción de la Decisión 2000/520/CE de 20 de julio de 2000 (en lo sucesivo la «Directiva sobre puerto seguro»). En esa Decisión, basada en el artículo 25, apartado 6, de la Directiva 95/46/CE[2], la Comisión otorgaba su reconocimiento a los principios de puerto seguro para la protección de la vida privada y a las preguntas más frecuentes correspondientes publicadas por el Departamento de Comercio de los Estados Unidos, como sistema capaz de garantizar una protección adecuada para los fines de transferencias de datos personales desde la UE[3]. Consiguientemente, los datos personales podían transferirse libremente de los Estados miembros de la UE a las empresas de los Estados Unidos que suscribieran dichos principios, a pesar de la inexistencia de una ley general de protección de datos en los Estados Unidos. El funcionamiento del régimen de puerto seguro se basaba en el compromiso y la autocertificación de las empresas que se adhiriesen a dichos principios. Si bien la adhesión a los principios de puerto seguro para la protección de la vida privada y a las preguntas más frecuentes correspondientes es voluntaria, esas normas son vinculantes, de conformidad con el

[1] Sentencia de 6 de octubre de 2015 en el asunto C-362/14 Maximilian Schrems / Data Protection Commissioner, UE:C:2015:650 (en lo sucesivo también: «la sentencia» o «la sentencia Schrems»).

[2] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23.11.1995, p. 31 (en lo sucesivo, «la Directiva 95/46/CE» o «la Directiva»).

[3] A efectos de la presente Comunicación, el término «UE» abarcará también el EEE. Se entenderá por lo tanto que las referencias a los «Estados miembros» incluyen también a los Estados miembros del EEE.

Derecho de los Estados Unidos, para quienes las hayan suscrito, siendo responsable del control de su cumplimiento la Comisión Federal de Comercio de los Estados Unidos[4].

En su sentencia de 6 de octubre de 2015, el Tribunal ha declarado inválida la Decisión sobre el puerto seguro. Ante esta circunstancia, el objetivo de la presente Comunicación es ofrecer una presentación general de los instrumentos alternativos para las transferencias transatlánticas de datos de conformidad con la Directiva 95/46/CE, a falta de una decisión de adecuación. La Comunicación también describe brevemente las consecuencias de la sentencia para otras decisiones de adecuación de la Comisión. En la sentencia, el Tribunal de Justicia aclara que toda decisión de adecuación adoptada de conformidad con el artículo 25, apartado 6, de la Directiva 95/46/CE está supeditada a la apreciación, por parte de la Comisión, de que existe en el tercer país correspondiente un nivel de protección de datos personales que, aunque no necesariamente idéntico, sea «sustancialmente equivalente» al que se garantiza en la UE en virtud de la Directiva, interpretada a la luz de la Carta de los Derechos Fundamentales. Por lo que respecta específicamente a la Decisión de puerto seguro, el Tribunal sostuvo que la Comisión no presentaba en ella suficientes datos sobre las limitaciones de acceso de las autoridades públicas de los Estados Unidos a los datos transferidos en virtud de dicha Decisión y a la existencia de una protección jurídica eficaz contra esa interferencia. En particular, el Tribunal explicitó que debía considerarse que toda legislación que permita a las autoridades públicas tener un acceso generalizado al contenido de las comunicaciones electrónicas compromete la esencia del derecho fundamental al respeto de la vida privada. Además, el Tribunal de Justicia confirmó que, incluso cuando exista una decisión de adecuación de conformidad con el artículo 25, apartado 6, de la Directiva 95/46/CE, las autoridades de protección de datos de los Estados miembros siguen estando facultadas y obligadas a examinar, con absoluta independencia, si las transferencias de datos a un tercer país se ajustan a los requisitos establecidos por la Directiva 95/46/CE, interpretado a la luz de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales. Sin embargo, también afirmó que solo el Tribunal de Justicia podía declarar inválido un acto de la UE, como una decisión de adecuación de la Comisión.

La sentencia del Tribunal de Justicia se inspira en la Comunicación de la Comisión de 2013 sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE[5], en el que la Comisión señalaba una serie de deficiencias y efectuaba 13 recomendaciones. Partiendo de estas recomendaciones, la Comisión ha venido manteniendo con las autoridades estadounidenses, desde enero de 2014, conversaciones dirigidas a implantar un régimen renovado e intensificado de intercambio transatlántico de datos.

---

[4] Para una descripción más detallada del régimen de puerto seguro, véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, COM/2013/847 final.

[5] Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, COM(2013) 847 final de 27.11.2013 Véanse también la Comunicación de la Comisión al Parlamento Europeo y al Consejo, «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.», COM(2013) 846 final, de 27.11.2013, y el Memorándum anexo, «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.: preguntas frecuentes», MEMO/13/1059 de 27.11.2013.

Tras la sentencia, la Comisión mantiene su compromiso con el objetivo de establecer un régimen renovado y sólido de transferencias transatlánticas de datos personales. Con tal fin, ha reanudado inmediatamente e intensificado su diálogo con el Gobierno de los EE.UU. para asegurarse de que todo nuevo régimen de transferencias transatlánticas de datos personales se ajuste plenamente a los parámetros establecidos por el Tribunal. Toda estructura creada con esos fines debe por consiguiente disponer de límites, salvaguardias y mecanismos de control judicial suficientes para asegurar una protección continuada de los datos personales de los ciudadanos de la UE, protegiéndolos también de un posible acceso a los mismos por parte de las autoridades públicas a efectos de la aplicación de la ley y de la seguridad nacional. Entretanto, las empresas del sector han expresado ciertas preocupaciones relacionadas con las posibilidades de continuidad de las transferencias de datos[6]. Es preciso, por lo tanto, aclarar las condiciones en las que pueden proseguir esas transferencias. Esa necesidad ha llevado al Grupo de Trabajo del artículo 29 (órgano consultivo independiente que reúne a representantes de todas las autoridades de protección de datos de los Estados miembros, así como al Supervisor Europeo de Protección de Datos) a emitir, el pasado 16 de octubre, una Declaración[7] sobre las primeras conclusiones que deben extraerse de la sentencia. Entre otros puntos, esa Declaración contenía las orientaciones siguientes sobre las transferencias de datos:

- las transferencias de datos no pueden ya basarse en la Decisión de puerto seguro de la Comisión, que ha sido invalidada;

- las cláusulas contractuales tipo (en lo sucesivo también «CCT» y las normas corporativas vinculantes (en lo sucesivo también «NCV») pueden utilizarse entre tanto como base para las transferencias de datos, aunque el Grupo de Trabajo del artículo 29 indicó también que seguiría analizando la repercusión de la sentencia en esos instrumentos alternativos.

En la Declaración se instaba también a los Estados miembros y a las instituciones de la UE a entablar conversaciones con las autoridades de los EE.UU. con vistas a encontrar soluciones jurídicas y técnicas para las transferencias de datos; las negociaciones sobre un nuevo régimen de puerto seguro podrían, en opinión del Grupo de Trabajo del artículo 29, formar parte de la solución.

---

6 Los representantes de las asociaciones industriales han manifestado sus preocupaciones, entre otros foros, en la reunión organizada al poco de dictarse la sentencia Schrems por el vicepresidente Ansip, la comisaria Jourová y el comisario Oettinger, el 14 de octubre. Véase el Daily News de 14.10.2015 (MEX/15/5840). Véase también: «Carta abierta sobre la ejecución de la sentencia del TJUE en el asunto C-362/14, Maximillian Schrems / Data Protection Commisioner», de 13 de octubre de 2015, dirigida al presidente de la Comisión, Jean-Claude Juncker, y firmada por diversas asociaciones industriales y empresas de la UE y de los EE.UU.: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353

7 Declaración del Grupo de Trabajo del artículo 29, que puede consultarse en Internet: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

El Grupo de Trabajo del artículo 29 anunció que si, a finales de enero de 2016 no se había encontrado una solución satisfactoria con las autoridades de los EE.UU. y en función de la evaluación de los instrumentos alternativos para las transferencias de datos, las autoridades de protección de datos tomarían todas las medidas necesarias y pertinentes, incluida una acción de ejecución coordinada.

Por último, el Grupo de Trabajo del artículo 29 insistió en la responsabilidad conjunta de las autoridades de protección de datos, las instituciones de la UE, los Estados miembros y las empresas para encontrar soluciones sostenibles que permitan aplicar la sentencia del Tribunal. Concretamente, el Grupo de Trabajo instó a las empresas a que se plantearan la posibilidad de poner en marcha cualquier solución jurídica y técnica capaz de mitigar los posibles riesgos a los que se enfrentan con las transferencias de datos.

La presente Comunicación se entiende sin perjuicio de las competencias y el deber de las autoridades de protección de datos de examinar la legalidad de esas transferencias con total independencia[8]. No establece normas vinculantes y respeta plenamente las competencias de los órganos jurisdiccionales nacionales para interpretar el Derecho vigente y, en su caso, plantear al Tribunal de Justicia una cuestión prejudicial. Tampoco puede constituir la base de ningún derecho o pretensión jurídica individuales o colectivos.

2. BASES ALTERNATIVAS PARA LAS TRANSFERENCIAS DE DATOS PERSONALES A LOS ESTADOS UNIDOS.

Las normas sobre transferencias internacionales de datos que establece la Directiva 95/46/CE se basan en una clara distinción entre, por una parte, las transferencias a terceros países que garanticen un nivel de protección adecuado (artículo 25 de la Directiva) y, por otra parte, las transferencias a terceros países respecto de los cuales no se haya confirmado que garanticen un nivel de protección adecuado (artículo 26 de la Directiva).

La sentencia Schrems aborda las condiciones en las que, de conformidad con el artículo 25, apartado 6, de la Directiva 95/46/CE, puede determinar la Comisión que un tercer país ofrece un nivel de protección adecuado.

Si se considera que el tercer país al que van a exportarse los datos personales desde la UE no garantiza ese nivel de protección adecuado, el artículo 26 de la Directiva 95/46/CE establece una serie de criterios alternativos sobre cuya base pueden efectuarse a pesar de todo las transferencias. Concretamente, las transferencias pueden realizarse cuando la entidad responsable de determinar los fines y medios del tratamiento de los datos personales (el «responsable del tratamiento»):

– ofrezca garantías suficientes, conforme a lo dispuesto en el artículo 26, apartado 2, de la Directiva 95/46/CE, respecto de la protección de la vida privada, los derechos y libertades

[8] Véanse el artículo 8, apartado 3, de la Carta de los Derechos Fundamentales de la UE y el artículo 16, apartado 2, del TFUE. El Tribunal de Justicia subraya también esta independencia en la sentencia Schrems.

fundamentales de las personas, así como respecto al ejercicio de tales derechos. Esas garantías pueden consistir, en particular, en cláusulas contractuales vinculantes entre el exportador y el importador de los datos (véanse las secciones 2.1 y 2.2). Dichas cláusulas incluyen las CCT fijadas por la Comisión y, en el caso de las transferencias entre las diferentes entidades de un grupo multinacional de empresas, las NCV autorizadas por los las autoridades de protección de datos; o

– se acoja a una de las excepciones expresamente recogidas en las letras a) a f) del artículo 26, apartado 1, de la Directiva 95/46/CE (véase la sección 2.3).

En comparación con las decisiones de adecuación que se derivan de la evaluación global del sistema de un tercer país determinado y pueden, en principio, cubrir todas las transferencias a ese sistema, estos criterios alternativos para las transferencias tienen a la vez un alcance más limitado (dado que solo se aplican a flujos de datos específicos) y una cobertura más amplia (puesto que no se circunscriben a ningún país en particular). Se aplican a los flujos de datos efectuados por determinadas entidades que han decidido hacer uso de alguna de las posibilidades ofrecidas por el artículo 26 de la Directiva 95/46/CE. Por otra parte, al realizar sus transferencias sobre esos criterios y dado que estas no pueden basarse en una constatación de la adecuación del tercer país recogida en una decisión de la Comisión, los exportadores y los importadores de datos asumen la responsabilidad de asegurar que las transferencias se ajustan a los requisitos de la Directiva.

2.1. Soluciones contractuales

Como destaca el Grupo de Trabajo del artículo 29, a fin de ofrecer garantías suficientes a efectos del artículo 26, apartado 2, de la Directiva 95/46/CE, las cláusulas contractuales deben compensar de manera satisfactoria la ausencia de una protección general adecuada, incluyendo los elementos esenciales de protección que no se den en una determinada situación concreta[9]. Para facilitar la utilización de esos instrumentos en las transferencias internacionales, la Comisión aprobó, de conformidad con el artículo 26, apartado 4, de la Directiva, cuatro conjuntos de CCT que considera cumplen los requisitos del artículo 26, apartado 2, de la Directiva. Dos de esos conjuntos de cláusulas tipo corresponden a las transferencias entre responsables del tratamiento[10], mientras que los otros dos se refieren a las transferencias entre un responsable y un encargado del tratamiento que actúe siguiendo las instrucciones del primero[11]. Cada uno de esos conjuntos de cláusulas tipo establece las

9 Véase: Grupo de Trabajo del artículo 29, «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos» (GT 12), 24 de julio de 1998, p. 16.

10 Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE, DO L 181 de 4.7.2001, p. 19, y Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de cláusulas contractuales tipo para la transferencia de datos personales a terceros países, DO L 385 de 29.12.2004, p. 74.

11 Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, 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, DO L 6 de 10.1.2002, p. 52, y Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo

obligaciones respectivas de los exportadores y los importadores. Las cláusulas incluyen obligaciones relativas, entre otros aspectos, a las medidas de seguridad, la información al interesado en caso de transferencia de datos sensibles, la notificación al exportador de datos de las solicitudes de acceso de las autoridades policiales y judiciales de terceros países o de todo acceso accidental o no autorizado, los derechos de acceso de los interesados al acceso, la rectificación y supresión de sus datos personales, así como las normas en materia de indemnización al interesado por los daños derivados de una vulneración de las CCT por cualquiera de las partes. Las cláusulas tipo exigen también que los interesados de la UE tengan la posibilidad de invocar ante una autoridad de protección de datos y/o un órgano jurisdiccional del Estado miembro en el que esté establecido el exportador de datos los derechos que para ellos dimanen de las cláusulas contractuales como terceros beneficiarios[12]. Las cláusulas contractuales deben necesariamente contener esos derechos y obligaciones, ya que, a diferencia de lo que sucede cuando la Comisión ha adoptado una decisión de adecuación, no puede presumirse que el importador de datos del tercer país esté sujeto a un sistema adecuado de supervisión y garantía de la aplicación de las normas de protección de datos.

Comoquiera que las decisiones de la Comisión son obligatorias en todos sus elementos en los Estados miembros, la incorporación de las CCT en un contrato significa que las autoridades nacionales están en principio obligadas a aceptarlas. Por consiguiente, no pueden denegar la transferencia de datos a un tercer país basándose únicamente en el argumento de que esas CCT no aportan las garantías suficientes. Esa imposibilidad se entiende sin perjuicio de la facultad de dichas autoridades para examinar las cláusulas con arreglo a los requisitos establecidos por el Tribunal de Justicia en la sentencia Schrems. En caso de duda, deberán someter el asunto a los órganos jurisdiccionales nacionales, los cuales podrán a su vez formular una petición de decisión prejudicial al Tribunal de Justicia. Si bien las leyes que incorporan la Directiva 95/45/CE en el ordenamiento jurídico de la mayor parte de los Estados miembros no incluyen el requisito de autorización nacional previa, algunos Estados miembros mantienen un sistema de notificación y/o autorización previa para el uso de CCT. En tales casos, la autoridad nacional de protección de datos ha de comparar las cláusulas efectivamente contenidas en el contrato en cuestión y comprobar que no se haya introducido en ellas ningún cambio[13]. Si las cláusulas se han utilizado sin modificación alguna[14], la

---

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, DO L 39 de 12.2.2010, p. 5. La primera decisión, derogada por la última, se aplica solo a los contratos celebrados antes del 15 de mayo de 2010.

12 Véanse, por ejemplo, el considerando 6 de la Decisión 2004/915/CE de la Comisión y la cláusula V de su anexo, así como la cláusula 7 del anexo de la Decisión 2010/87/UE de la Comisión.

13 Procede señalar que la propuesta de Reglamento general de protección de datos (COM(2012) 11 final) prevé que las transferencias basadas en CCT o en NCV, en la medida en que estas hayan sido adoptadas por la Comisión o de acuerdo con el mecanismo de coherencia previsto, no requerirán autorización suplementaria.

14 El uso de las CCT no impide, sin embargo, a las partes acordar la inserción de cláusulas adicionales, siempre que no contradigan directa o indirectamente a las cláusulas aprobadas por la Comisión ni prejuzguen los derechos fundamentales y las libertades de los interesados. Véase: Comisión Europea, «Preguntas frecuentes relativas a las transferencias de datos personales de la UE/EEE a terceros países» (Preguntas frecuentes B. 1.9), p. 28 (disponible en la siguiente dirección de Internet: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

autorización se concede, en principio[15], automáticamente[16]. Conforme se explica más adelante (véase la sección 2.4), todas estas disposiciones se entienden sin perjuicio de las medidas adicionales que el exportador de datos pueda tener que adoptar, sobre todo en caso de que el importador de datos le proporcione información que indique la introducción de cambios en el sistema jurídico del tercer país que puedan impedirle cumplir las obligaciones derivadas del contrato. Para la aplicación de las CCT, tanto los exportadores de datos como, tras su adhesión al contrato, los importadores de datos están sujetos a la supervisión de las autoridades de protección de datos.

La adopción de CCT no impide a las empresas recurrir a otros instrumentos, como disposiciones contractuales *ad hoc*, para demostrar que sus transferencias se efectúan con las garantías suficientes conforme exige el artículo 26, apartado 2, de la Directiva 95/46/CE. De conformidad con el artículo 26, apartado 2, de la Directiva, cada uno de estos instrumentos debe ser aprobados por las autoridades nacionales. Algunas autoridades de protección de datos han elaborado directrices este ámbito, en forma incluso de contratos tipo o normas detalladas que deben seguirse para redactar las cláusulas de transferencia de datos. La mayor parte de los contratos actualmente utilizados por las empresas para llevar a cabo sus transferencias internacionales de datos se basan, no obstante, en las CCT aprobadas por la Comisión[17].

2.2. Transferencias dentro de un mismo grupo

Una empresa multinacional puede adoptar NCV para transferir datos personales desde la UE a sus filiales situadas fuera de la UE con arreglo a los requisitos establecidos en el artículo 26, apartado 2, de la Directiva 95/46/CE. Este tipo de código de prácticas sienta únicamente las bases para las transferencias efectuadas dentro de un mismo grupo de empresas.

El uso de NCV posibilita por lo tanto la libre circulación de datos personales entre las diversas entidades de un grupo de empresas en todo el mundo, lo que evita la necesidad de establecer disposiciones contractuales entre todas y cada una de esas entidades, ofreciendo al mismo tiempo un idéntico y elevado nivel de protección de los datos personales a todos los miembros del grupo mediante un único conjunto de normas de carácter vinculante y ejecutivo. El conjunto único de normas supone un régimen más sencillo y más eficaz, más fácil de

[15] Si alguna autoridad de protección de datos alberga dudas acerca de la compatibilidad de las CCT con los requisitos de la Directiva, debe someter la cuestión a un órgano jurisdiccional nacional, el cual puede plantear una cuestión prejudicial al Tribunal de Justicia (véanse los apartados 51, 52, 64 y 65 de la sentencia Schrems).

[16] El Grupo de Trabajo del artículo 29 ha establecido un procedimiento de cooperación específico entre autoridades de protección de datos para la aprobación de cláusulas contractuales que una empresa pretenda utilizar en distintos Estados miembros. Grupo de Trabajo del artículo 29, «Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause» (GT 226) de 26 de noviembre de 2014. Véanse también la cláusula VII del anexo de la Decisión 2004/915/CE de la Comisión y la cláusula 10 del anexo de la Decisión 2010/87/UE de la Comisión.

[17] Véase: Grupo de Trabajo del artículo 29, «Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause» (GT 226) de 26 de noviembre de 2014, p. 2.

aplicar para el personal responsable y más fácil de comprender para los interesados. Para ayudar a las empresas a redactar las NCV, el Grupo de Trabajo del artículo 29 ha definido sus requisitos sustantivos (por ejemplo, limitación de los fines, seguridad del tratamiento, transparencia de la información a los interesados, restricciones de las transferencias posteriores fuera del grupo, derechos de acceso, rectificación y oposición, etc.) y procedimentales (por ejemplo, auditorías, control del cumplimiento, tramitación de las reclamaciones, cooperación con las autoridades de protección de datos, responsabilidad y jurisdicción) basándose en las normas de protección de datos de la UE[18]. Además de ser vinculantes para los miembros del grupo de empresas, esas normas, al igual que las CCT, tienen carácter ejecutivo en la UE: las personas cuyos datos estén siendo tratados por una entidad del grupo podrán, como terceros beneficiarios, exigir el cumplimiento de las NCV mediante la presentación de una reclamación ante una autoridad de protección de datos y la interposición de la correspondiente acción ante un tribunal de un Estado miembro. Además, las NCV deben designar una entidad dentro de la UE que asuma la responsabilidad por el incumplimiento de las normas por parte de cualquier miembro del grupo situado fuera de la UE que esté vinculado por dichas normas.

Conforme a las leyes por las que la mayor parte de los Estados miembros incorporan la Directiva, las transferencias de datos efectuadas con arreglo a NCV han de ser autorizadas por la autoridad de protección de datos de cada Estado miembro desde el que la empresa multinacional tenga la intención de transferir los datos. Para facilitar y acelerar el proceso, reduciendo además las cargas para los solicitantes, el Grupo de Trabajo del artículo 29 ha elaborado un formulario de solicitud normalizado[19] y un procedimiento específico de cooperación entre autoridades de protección de datos afectadas[20] que incluye la designación de una «autoridad principal» responsable de tramitar el procedimiento de aprobación.

2.3. Excepciones

A falta de una decisión de adecuación con arreglo al artículo 25, apartado 6, de la Directiva 95/46/CE y con independencia de la utilización de CCT y/o NCV, los datos personales podrán transferirse a entidades establecidas en un tercer país siempre que sea aplicable alguna de las excepciones alternativas establecidas en el artículo 26, apartado 1, de la Directiva 95/46/CE[21]:

---

18 Véase: Grupo de Trabajo del artículo 29, «Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules» (GT 153), 24 de junio de 2008; «Working Document setting up a framework for the structure of Binding Corporate Rules» (GT 154), 24 de junio de 2008 y «Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules» (GT 155), 24 de junio de 2008.

19 Grupo de Trabajo del artículo 29, «Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data» (GT 133), 10 de enero de 2007.

20 Grupo de Trabajo del artículo 29, «Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From Binding Corporate Rules» (GT 107), 14 de abril de 2005.

21 Como ha subrayado el Grupo de Trabajo del artículo 29, en la medida en que otras disposiciones de la Directiva 95/46/CE incluyan requisitos adicionales pertinentes para el uso de estas excepciones (por ejemplo, las limitaciones del artículo 8 para el tratamiento de datos sensibles), estos deben respetarse. Véase: Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995», 25 de noviembre de 2005, p, 8.

– el interesado ha dado su consentimiento inequívoco a la transmisión propuesta;

– la transmisión es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la aplicación de medidas precontractuales a petición del interesado;

– la transmisión es necesaria para la conclusión o ejecución de un contrato celebrado en beneficio del interesado entre el responsable del tratamiento y un tercero;

– la transmisión es necesaria o legalmente obligatoria por razones importantes de interés público[22] o para el establecimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial;

– la transmisión es necesaria para proteger intereses vitales del interesado;

– la transferencia tiene lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

Estos motivos justifican la excepción a la prohibición general de transferir datos personales a entidades establecidas en un tercer país sin un nivel de protección adecuado. De hecho, el exportador de datos no tiene que garantizar que el importador de datos vaya a dispensar la protección adecuada, y en principio no necesitará obtener de las autoridades nacionales competentes autorización previa para la transferencia. No obstante, debido a su carácter excepcional, el Grupo de Trabajo del artículo 29 considera que dichos supuestos de inaplicación deben ser objeto de una interpretación estricta[23].

El Grupo de Trabajo del artículo 29 ha publicado diversos documentos de orientación no vinculantes sobre la aplicación del artículo 26, apartado 1, de la Directiva 95/46/CE[24]. Entre

---

Véase también: Comisión Europea, «Preguntas frecuentes relativas a las transferencias de datos personales de la UE/EEE a terceros países» (Preguntas frecuentes D.2), p. 50

22 Este supuesto puede incluir, por ejemplo, las transferencias de datos entre autoridades fiscales o aduaneras, o entre servicios competentes en materia de seguridad social (véase el considerando 58 de la Directiva 95/46/CE). Pueden acogerse también a la excepción las transferencias entre organismos de supervisión del sector de los servicios financieros. Véase: Grupo de Trabajo del artículo 29, «Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos» (GT 12), 24 de julio de 1998, p. 25.

23 Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995», (GT 114), 25 de noviembre de 2005, pp. 7 y 17.

24 Grupo de Trabajo del artículo 29, «Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos» (GT 12), 24 de julio de 1998; «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005. Véase también:

ellos se incluye una serie de reglas de «mejores prácticas» dirigidas a encauzar la actividad de ejecución de las autoridades de protección de datos[25]. En particular, el Grupo de Trabajo recomienda que las transferencias de datos personales que puedan calificarse de repetidas, masivas o estructurales se lleven a cabo con las garantías suficientes y, en la medida de lo posible, dentro de un marco jurídico específico como las CCT o las NCV[26].

En la presente Comunicación, la Comisión hará solo referencia a las excepciones que resultan especialmente pertinentes para las transferencias en el contexto comercial tras la declaración de invalidez de la Decisión sobre el puerto seguro.

2.3.1. Transferencias necesarias para la ejecución de un contrato o la aplicación de medidas precontractuales adoptadas en respuesta a la solicitud del interesado [artículo 26, apartado 1, letra b)]

Esta excepción podría ser aplicable, por ejemplo, en relación con una reserva de hotel o cuando se transfiera a un tercer país información sobre pagos para efectuar una transferencia bancaria. Sin embargo, en cada uno de estos casos, el Grupo de Trabajo del artículo 29 considera que debe existir un «vínculo estrecho y sustancial», «una relación directa y objetiva» entre el interesado y el objeto del contrato o de las medidas precontractuales (prueba de necesidad)[27]. Además, la excepción no puede aplicarse a las transferencias de información adicional que no sea necesaria para la transferencia, o a las transferencias destinadas a un fin distinto de la ejecución del contrato (por ejemplo, comercialización de seguimiento)[28]. Por lo que se refiere a las medidas precontractuales, el Grupo de Trabajo del artículo 29 consideró que solo estarían cubiertos los contactos iniciados por el interesado (por ejemplo, una solicitud de información sobre un determinado servicio), pero no los resultantes de las estrategias de comercialización adoptadas por el responsable del tratamiento de los datos[29].

Comisión Europea, «Preguntas frecuentes relativas a las transferencias de datos personales de la UE/EEE a terceros países» (Preguntas frecuentes D.1 a D.9), pp. 48-54.

[25] Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, pp., 8-10.

[26] Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p, 9. Según el Grupo de Trabajo, las transferencias masivas o repetidas solo podrán efectuarse al amparo de una excepción cuando el recurso a las CCT o a las NCV resulte imposible en la práctica y cuando los riesgos para los interesados sean mínimos (por ejemplo, transferencias de dinero internacionales). Véase también: Comisión Europea, «Preguntas frecuentes relativas a las transferencias de datos personales de la UE/EEE a terceros países» (Preguntas frecuentes D.2), p. 49.

[27] Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p, 13. Véase también el «Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos» (GT 66), 24 de octubre de 2002.

[28] Grupo de Trabajo del artículo 29, «Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos (GT 12), 24 de julio de 1998, p. 24; «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p. 13.

[29] Grupo de Trabajo del artículo 29, «Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos» (GT 12), 24 de julio de 1998, p. 24.

2.3.2. Transferencias necesarias para la celebración o ejecución de un contrato celebrado en interés del interesado entre el responsable del tratamiento o un tercero [artículo 26, apartado 1, letra c)]

Esta excepción podría ser aplicable, por ejemplo, cuando el interesado sea beneficiario de una transferencia bancaria internacional, o cuando una agencia de viajes envíe los pormenores de una reserva de vuelo a una compañía aérea. Una vez más, debe aplicarse la prueba de necesidad para demostrar, en este caso, la existencia de un vínculo estrecho y sustancial entre el interés del interesado y el fin perseguido con el contrato.

2.3.3. Transferencias necesarias u obligatorias desde un punto de vista legal para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial [artículo 26, apartado 1, letra d)]

Esta excepción podría ser aplicable, por ejemplo, cuando una empresa necesite transferir datos para defenderse frente a una reclamación legal, o para presentar una reclamación ante un órgano jurisdiccional o una autoridad pública. Como las dos excepciones anteriores, está sujeta a la prueba de necesidad:[30] debe darse una estrecha relación con procedimientos contenciosos o judiciales (incluidos los de orden administrativo).

Según el Grupo de Trabajo del artículo 29, la excepción solo puede aplicarse si se han cumplido normas internacionales en materia de cooperación en procesos penales o civiles que regulen ese tipo de transferencia, en particular las que se deriven de las disposiciones del Convenio de La Haya de 18 de marzo de 1970 (Convenio sobre «obtención de pruebas»)[31].

2.3.4. Consentimiento previo inequívoco del interesado a la transferencia propuesta [artículo 26, apartado 1, letra a),]

Si bien es cierto que el consentimiento puede tomarse como base de las transferencias de datos, es preciso tener en cuenta una serie de consideraciones. El hecho de que el consentimiento deba otorgarse a la transferencia «propuesta» exige el consentimiento previo para cada transferencia concreta (o para cada categoría específica de transferencias). Si este consentimiento se solicita en línea, el Grupo de Trabajo del artículo 29 recomienda la utilización de casillas que deban marcarse (en lugar de casillas previamente marcadas)[32].

---

30 Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p, 15. Por ejemplo, en un contexto laboral, la excepción no puede utilizarse para transferir todos los expedientes de los empleados a la empresa matriz del grupo establecida en un tercer país alegando posibles acciones legales futuras.

31 Convenio de la Haya sobre la Obtención de Pruebas en el Extranjero en Materia Civil o Comercial, *abierto a la firma* el 18 de marzo de 1970, 23 U.S.T. 2555, 847 U.N.T.S. 241. Dicho Convenio incluye, por ejemplo, la aportación preliminar de pruebas (*pre-trial discovery*) o la solicitud de las autoridades judiciales de un Estado a la autoridad competente de otro que obtenga pruebas para su utilización en procedimientos judiciales en el Estado requirente.

32 Grupo de trabajo del artículo 29, «Documento de trabajo sobre una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p. 10, con referencia al «Dictamen 5/2004 sobre comunicaciones de venta directa no solicitadas de conformidad con el artículo 13 de la Directiva 2002/58/CE» (GT 90), 27 de febrero de 2004, punto 3.2.

Dado que el consentimiento ha de ser inequívoco, cualquier duda sobre su otorgamiento efectivo haría inaplicable esta excepción. Esto significará, probablemente, que muchas situaciones en las que el consentimiento se da por supuesto (por ejemplo, porque la persona ha sido informada de una transferencia y no se ha opuesto a ella), no pueden ser objeto de la excepción. A la inversa, la excepción podría aplicarse en aquellos casos en que la entidad cedente tenga contacto directo con el interesado y pueda proporcionarse fácilmente la información necesaria y obtenerse un consentimiento inequívoco[33].

Por otra parte, según el artículo 2, letra h), de la Directiva 95/46/CE, el consentimiento debe ser libre, específico e informado. Según el Grupo de Trabajo del artículo 29, el primer requisito implica que cualquier «presión» puede invalidar el consentimiento. Esta circunstancia resulta especialmente pertinente en el contexto laboral, donde la relación de subordinación e inherente dependencia de los empleados suscitará por lo general dudas sobre la idoneidad del consentimiento[34]. En términos más generales, el consentimiento otorgado por un interesado que no haya tenido la oportunidad de hacer una auténtica elección o que haya sido puesto frente a un hecho consumado no puede considerarse válido[35].

Tiene gran importancia que se notifique con antelación a los interesados que los datos pueden transferirse fuera de la UE, a qué terceros países y en qué condiciones (finalidad, identidad y datos pormenorizados de los destinatarios, etc.). Esta información deberá cubrir el riesgo específico de que dichos datos vayan a transferirse a un tercer país carente de la protección adecuada[36]. Además, como ha señalado el Grupo de Trabajo del artículo 29, la retirada del consentimiento del interesado, si bien no tiene carácter retroactivo, debe por principio, descartar cualquier tratamiento posterior de datos personales[37]. Habida cuenta de estas limitaciones, el Grupo de Trabajo del artículo 29 considera improbable que el consentimiento ofrezca a los responsables del tratamiento un marco adecuado a largo plazo en casos de transferencias estructurales[38].

---

33 Grupo de Trabajo del artículo 29, «Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos» (GT 12), 24 de julio de 1998, p. 24.

34 Grupo de Trabajo del artículo 29, «Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto del empleo (GT 48), 13 de septiembre de 2001, pp. 3, 23 y 26. Según el Grupo de Trabajo, la supeditación al consentimiento debe ceñirse a los casos en los que el trabajador tenga una auténtica libertad de elección y pueda por lo tanto revocar posteriormente su consentimiento sin perjuicio alguno. Véase también: Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995», (GT 114), 25 de noviembre de 2005, p, 11.

35 Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p, 11. Véase también el «Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos» (GT 66), 24 de octubre de 2002.

36 Grupo de Trabajo del artículo 29, «Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos» (GT 12), 24 de julio de 1998, p. 24.

37 Grupo de Trabajo del artículo 29, «Dictamen 15/2011 sobre la definición del consentimiento» (GT 187), 13 de julio de 2011, p. 9.

38 Grupo de Trabajo del artículo 29, «Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995» (GT 114), 25 de noviembre de 2005, p, 11.

2.4. Resumen de las bases alternativas para las transferencias de datos personales

Se desprende de todo lo anterior que las empresas pueden usar diferentes instrumentos alternativos para llevar a cabo las transferencias internacionales de datos a terceros países que no demuestren garantizar un nivel de protección adecuado a tenor del artículo 25, apartado 2, de la Directiva 95/46/CE. A raíz de la sentencia Schrems, el Grupo de Trabajo del artículo 29 ha aclarado, entre otras cuestiones, que las CCT y las NCV pueden utilizarse, mientras prosigue su evaluación, para transferir datos a los EE.UU., sin menoscabo de las facultades de las autoridades de protección de datos para investigar casos concretos[39]. Las reacciones de la industria del sector a la sentencia han sido muy diversas y también lo han sido lo que respecta a la opción de basar sus transferencias de datos en esos instrumentos alternativos[40].

No obstante, es preciso destacar dos condiciones importantes: En primer lugar, debe recordarse que, independientemente de la base jurídica invocada, las transferencias a un tercer país solo pueden hacerse dentro de la legalidad si los datos han sido originalmente recogidos y posteriormente tratados por el responsable del tratamiento de datos establecido en la UE de conformidad con las leyes nacionales vigentes que incorporen la la Directiva 95/46/CE. La Directiva especifica expresamente que la actividad de transformación previa a la transferencia y la propia transferencia han de ajustarse plenamente a las normas adoptadas por los Estados miembros con arreglo a las demás disposiciones de la Directiva[41]. En segundo lugar, a falta de una declaración de adecuación de la Comisión, los responsables del tratamiento son quienes deben asegurar que sus transferencias de datos se efectúen con las salvaguardias suficientes conforme al artículo 26, apartado 2, de la Directiva. Esa valoración debe llevarse a cabo en relación con todas las circunstancias que concurran en torno a la transferencia de que se trate. En particular, tanto las CCT como las NCV establecen que si el importador de datos tiene motivos para creer que la legislación vigente en el país beneficiario puede impedirle el cumplimiento de sus obligaciones, debe comunicar sin demora esa información al exportador de datos en la UE. En tales situaciones, es el exportador quien debe considerar la posibilidad de adoptar las disposiciones apropiadas para garantizar la protección de los datos personales[42]. Estas disposiciones pueden abarcar desde medidas técnicas, organizativas, relativas al modelo

---

39 Véase la Declaración del Grupo de Trabajo del artículo 29 de 16 de octubre de 2015 (citada en la nota a pie de página 8).

40 Algunas empresas multinacionales han declarado que basan sus transferencias de datos a Estados Unidos de datos en los instrumentos alternativos. Véanse, por ejemplo, las declaraciones de Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) o Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). Otras empresas de los Estados Unidos, como Oracle, han indicado que ofrecen a los clientes de los servicios de nube la posibilidad de almacenar sus datos en Europa a fin de evitar que se envíe, para su almacenamiento, a otro lugar: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

41 Véanse el considerando 60 y el artículo 25, apartado 1, de la Directiva 95/46/CE.

42 Véase, por ejemplo, la cláusula 5 del anexo de la Decisión 2010/87/UE de la Comisión, y el documento del Grupo de Trabajo del artículo 29, «Working Document setting up a framework for the structure of Binding Corporate Rules» (GT 154), 24 de junio de 2008, p. 8.

de negocio o legales[43] hasta la posibilidad de suspender la transferencia de datos o de rescindir el contrato. Teniendo en cuenta todas las circunstancias de la transferencia, los exportadores de datos pueden por lo tanto verse en la necesidad de aplicar salvaguardias adicionales que completen las dispensadas por las bases jurídicas aplicables a las transferencias a fin de cumplir los requisitos del artículo 26, apartado 2, de la Directiva.

El cumplimiento de esos requisitos deberán, en último término, evaluarlo en cada caso las autoridades de protección de datos tanto en el ejercicio de sus funciones de supervisión y ejecución (incluso en el marco de la aprobación de los acuerdos contractuales y las NCV), como en respuesta a las reclamaciones individuales. Si bien algunas autoridades de protección de datos han expresado sus dudas acerca de la posibilidad de utilizar instrumentos de transferencia como las CCT o las NCV para los flujos de datos transatlánticos[44], en la declaración emitida a raíz de la sentencia Schrems, el Grupo de Trabajo del artículo 29 anunció que continuaría su análisis del impacto de la sentencia en otros instrumentos de transferencia[45]. Sin perjuicio de las facultades de las autoridades de protección de datos para investigar casos concretos y de ejercer sus competencias con miras a la protección de personas.

3. CONSECUENCIAS DE LA SENTENCIA SCHREMS EN LAS DECISIONES DE ADECUACIÓN

En su sentencia, el Tribunal de Justicia no pone en tela de juicio las competencias que el artículo 25, apartado 6, de la Directiva 95/46/CE confiere a la Comisión para declarar que un tercer país garantiza un nivel de protección adecuado, siempre que se cumplan los requisitos establecidos por el Tribunal de Justicia. En consonancia con esos requisitos, la propuesta de 2012 relativa a un Reglamento general sobre protección de datos[46] en sustitución de la

[43] Véanse, por ejemplo, las orientaciones emitidas por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

[44] Véase, por ejemplo, el documento de posición emitido por la Conferencia de protección de datos de las autoridades alemanas de protección de datos a nivel federal y estatal de 26.10.2015: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Subrayando que la sentencia Schrems contiene «estrictos requisitos sustantivos» que tanto la Comisión como las autoridades de protección de datos deben respetar, el documento de posición indica que las autoridades de protección de datos alemanas estudiarán la legalidad de las transferencias de datos basadas en instrumentos alternativos (CCT y NCV) y dejarán de conceder nuevas autorizaciones para el uso de esos instrumentos. De forma paralela, algunas autoridades de protección de datos alemanas han emitido claras advertencias de que los instrumentos de transferencia alternativos están bajo escrutinio jurídico. Véanse, por ejemplo, los documentos de posición publicados por las autoridades de protección de datos de Schleswig-Holstein:https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html y de Renania-Palatinado: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

[45] Véase la Declaración del Grupo de Trabajo del artículo 29 de 16 de octubre de 2015 (nota a pie de página 8).

[46] Comisión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) Véase también: Parlamento Europeo, Resolución legislativa de 12 de marzo de 2014 sobre la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la

Directiva 95/46/CE aclara y precisa las condiciones en las que pueden adoptarse decisiones de adecuación. En la sentencia Schrems, el Tribunal de Justicia aclara también que cuando la Comisión adopta una decisión de adecuación, esta es vinculante para todos los Estados miembros y sus órganos, incluidas las autoridades de protección de datos, en tanto no haya sido revocada, anulada o declarada inválido por el Tribunal de Justicia, único organismo competente a ese respecto. Las autoridades de protección de datos conservan su competencia para examinar las solicitudes en el sentido del artículo 28, apartado 4, de la Directiva 95/46/CE y comprobar que la transferencia de datos se ajusta a los requisitos de la Directiva (conforme a la interpretación del Tribunal de Justicia), pero no pueden formular conclusiones definitivas. Por el contrario, los Estados miembros han de prever la posibilidad de someter el asunto a un órgano jurisdiccional nacional, el cual puede a su vez invocar la competencia del Tribunal de Justicia mediante una petición de decisión prejudicial con arreglo al artículo 267 del Tratado de Funcionamiento de la Unión Europea (TFUE).

Por otra parte, el Tribunal de Justicia confirmó expresamente que el recurso por parte de un tercer país a un sistema de autocertificación (como el correspondiente a los principios de puerto seguro para la protección de la vida privada) no excluye una decisión de adecuación con arreglo al artículo 25, apartado 6, de la Directiva 95/46/CE, en la medida en que existen mecanismos eficaces de detección y supervisión que permiten, en la práctica, detectar y sancionar las infracciones de las normas de protección de datos.

Como la Decisión de puerto seguro no contenía suficientes constataciones en este sentido, el Tribunal de Justicia dictaminó su invalidez. Queda por lo tanto claro que las las transferencias de datos entre la UE y los Estados Unidos no pueden ya efectuarse sobre esa base, es decir, invocando únicamente la adhesión a los principios de puerto seguro para la protección de la vida privada. Dado que las transferencias de datos a un tercer país que no garantice un nivel de protección adecuado (o, al menos, respecto del que no se haya confirmado esa garantía de protección mediante una decisión de la Comisión conforme al artículo 25, apartado 6, de la Directiva 95/46/CE) están, en principio, prohibidas[47], solo se considerarán legales si el exportador de datos puede recurrir a uno de los instrumentos alternativos descritos en la sección 2 anterior. A falta de una decisión de adecuación, es responsabilidad del exportador de datos, bajo el control de las autoridades de protección de datos, garantizar que se cumplan las condiciones para recurrir a (uno de) esos instrumentos para la transferencia de datos correspondiente.

El alcance de la sentencia se limita a la Decisión sobre el régimen de puerto seguro de la Comisión. No obstante, cada una de las demás decisiones de adecuación[48] contiene una

---

libre circulación de estos datos (Reglamento general de protección de datos) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); Consejo, Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), Preparación de un enfoque general, 9565/15. La propuesta se encuentra actualmente en la fase final del proceso legislativo.

47 Véase el considerando 57 de la Directiva 95/46/CE.

48 Hasta la fecha, se han adoptado decisiones de adecuación con respecto a los siguientes países: Andorra, Argentina, Canadá, Guernsey, Islas Feroe, Isla de Man, Israel, Jersey, Nueva Zelanda, Suiza y Uruguay. Véase: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

limitación de las competencias de las autoridades de protección de datos que es idéntica al artículo 3 de la Decisión sobre el régimen de puerto seguro, considerada inválida por el Tribunal de Justicia[49]. La Comisión extraerá ahora las consecuencias oportunas de la sentencia y preparará en breve una decisión, que se aplicará conforme al procedimiento de comitología aplicable, que sustituirá dicha disposición en todas las decisiones de adecuación. Además, la Comisión emprenderá una evaluación regular de las decisiones de adecuación existentes y futuras, consistente entre otras cosas en la revisión periódica de su funcionamiento conjuntamente con las autoridades competentes del tercer país de que se trate.

4. CONCLUSIÓN

Según confirmó el Grupo de Trabajo del artículo 29, las empresas pueden seguir utilizando instrumentos alternativos que autoricen flujos de datos para efectuar transferencias legales de datos a terceros países como los Estados Unidos. No obstante, la Comisión considera absolutamente prioritario el establecimiento de un marco renovado y sólido para las transferencias de datos personales a los Estados Unidos. Un marco de esas características es la solución más general para asegurar la efectiva continuidad de la protección de los datos personales de los ciudadanos europeos cuando se transfieran a los Estados Unidos. También supone la mejor solución para el comercio transatlántico, ya que ofrece un mecanismo de transferencia más sencillo, menos engorroso y, por tanto, menos gravoso, especialmente para las pymes.

Ya en 2013, la Comisión entabló negociaciones con el Gobierno de los EE.UU. encaminadas a acordar un nuevo régimen de transferencias transatlánticas de datos basado en sus 13 recomendaciones[50]. Se han dado grandes pasos para acercar los puntos de vista de ambas partes en lo que respecta, por ejemplo, a la mejora del control y la observancia de los principios de puerto seguro para la protección de la vida privada por, respectivamente, el Departamento de Comercio de los Estados Unidos y la Comisión de Comercio Federal de los EE.UU., el aumento de la transparencia para los consumidores en cuanto a sus derechos de protección de datos, las vías más fáciles y baratas de recurso en caso de reclamación y las normas más claras en materia de transferencias ulteriores desde «empresas de puerto seguro» hacia empresas que no reúnan esas condiciones (con fines, por ejemplo, de tratamiento o subtratamiento). Ahora que la Decisión sobre el régimen de puerto seguro ha sido declarada inválida, la Comisión ha intensificado el diálogo con el Gobierno de los EE.UU. para garantizar el cumplimiento de los requisitos jurídicos formulados por el Tribunal. El objetivo de la Comisión es concluir estas conversaciones y lograr este objetivo en tres meses.

Hasta que se implante el marco transatlántico renovado, las sociedades deberán recurrir a los instrumentos de transferencia alternativos disponibles. No obstante, esa opción implica responsabilidades para los exportadores de datos, bajo la supervisión de las autoridades de protección de datos.

---

49 Véanse los apartados 99 a 104 de la sentencia Schrems.

50 Véase la nota a pie de página 4.

A diferencia de la situación en la que la Comisión considera que un tercer país garantiza un nivel adecuado de protección de datos, en la que pueden basarse los exportadores de datos para las transferencias de datos desde la UE, éstos mantienen la responsabilidad de verificar la efectiva protección de los datos de carácter personal al utilizar los instrumentos alternativos. Para ello, pueden tener que adoptar medidas apropiadas en caso necesario.

A tal respecto, las autoridades de protección de datos desempeñan un papel fundamental. Como principales garantes del respeto de los derechos fundamentales de los interesados, las autoridades de protección de datos son responsables y competentes para supervisar las transferencias de datos de la UE hacia terceros países, con total independencia. La Comisión invita a los responsables del tratamiento de datos a que cooperen con las autoridades de protección de datos, ayudándolas así a desempeñar con eficacia sus funciones de supervisión. La Comisión seguirá colaborando estrechamente con el Grupo de Trabajo del artículo 29 para garantizar una aplicación uniforme de la normativa de protección de datos de la UE.