

Preguntas frecuentes sobre la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 – Data Protection Commissioner contra Facebook Ireland Ltd y Maximilian Schrems

Adoptado el 23 de julio de 2020

(Traducción no oficial)

Este documento tiene por objeto presentar respuestas a algunas preguntas frecuentes recibidas por las autoridades de supervisión (Agencias de Protección de Datos) y se desarrollará y complementará junto con un análisis más detallado, ya que el Comité Europeo de Protección de Datos (CEPD) continúa examinando y evaluando la sentencia del Tribunal de Justicia de la Unión Europea (el «Tribunal»).

La sentencia C-311/18 puede encontrarse en el siguiente enlace---, y el comunicado de prensa del Tribunal de Justicia puede encontrarse en el enlace---

1) ¿Qué dictaminó el Tribunal en su sentencia?

- ➔ En su sentencia, el Tribunal de Justicia examina la validez de la Decisión 2010/87/CE de la Comisión Europea sobre las cláusulas contractuales estándar («CCE») y considera que ésta es válida. De hecho, la validez de dicha decisión no se pone en tela de juicio por el mero hecho de que las cláusulas tipo de protección de datos de dicha decisión no vinculan, dado su carácter contractual, a las autoridades del tercer país al que pueden transferirse los datos.

No obstante, dicha validez, añade el Tribunal de Justicia, depende de que la Decisión 2010/87/CE incluya mecanismos eficaces que permitan, en la práctica, garantizar el cumplimiento un nivel de protección “*esencialmente equivalente*” al garantizado en la UE por el RGPD y de que las transferencias de datos personales en virtud de dichas cláusulas se suspendan o prohíban en caso de incumplimiento de o de la imposibilidad de respetarlas.

A este respecto, el Tribunal de Justicia señala, en particular, que la Decisión 2010/87/CE impone al exportador de datos y al destinatario de los datos (el

«importador de datos») la obligación de verificar, antes de cualquier transferencia, y teniendo en cuenta las circunstancias de la transferencia, si ese nivel de protección se respeta en el tercer país de que se trate, y que la Decisión 2010/87/CE exige al importador de datos que informe al exportador de cualquier incapacidad para cumplir las cláusulas estándar de protección de datos (CCE) y, en su caso, de las “medidas suplementarias” a las ofrecidas por las cláusulas, estando en su caso obligado a suspender la transferencia de los datos o rescindir el contrato con el importador.

- ➔ El Tribunal también ha examinado la validez de la Decisión sobre el Escudo de Privacidad (Decisión 2016/1250 sobre la adecuación de la protección proporcionada por el Escudo de Privacidad UE-Estados Unidos), ya que las transferencias en juego en el contexto del litigio nacional ante el tribunal irlandés que dio lugar a la solicitud de decisión prejudicial tuvieron lugar entre la UE y los Estados Unidos («Estados Unidos»).

El Tribunal ha considerado que los requisitos de la legislación nacional de los Estados Unidos, y en particular algunos programas de vigilancia que permiten el acceso de las autoridades públicas de los Estados Unidos a los datos personales transferidos desde la UE a los Estados Unidos con fines de seguridad nacional, dan lugar a limitaciones a la protección de los datos personales que no están circunscritas de manera que satisfagan requisitos que son esencialmente equivalentes a los exigidos por la legislación de la UE¹, y que esta legislación no otorga derechos recurribles ante los tribunales contra las autoridades de los Estados Unidos.

Como consecuencia de tal grado de injerencia en los derechos fundamentales de las personas cuyos datos se transfieren a ese tercer país, el Tribunal declaró inválida la Decisión de adecuación del Escudo de Privacidad.

2) ¿El fallo de la Corte tiene implicaciones en las herramientas de transferencia distintas del Escudo de Privacidad?

- ➔ En general, en el caso de terceros países, el umbral establecido por el Tribunal se aplica también a todas las salvaguardias adecuadas con arreglo al artículo 46 del RGPD utilizadas para transferir datos del Espacio Económico Europeo (EEE) a cualquier tercer país. La legislación estadounidense mencionada por el Tribunal (es decir, la sección 702 de la FISA y la EO 12333) se aplica a cualquier transferencia a los Estados Unidos por medios electrónicos que entren en el ámbito de aplicación de esta legislación, independientemente del instrumento de transferencia utilizado para la transferencia².

¹ El Tribunal subraya que determinados programas de vigilancia que permiten el acceso de las autoridades públicas de los Estados Unidos a los datos personales transferidos de la UE a los Estados Unidos con fines de seguridad nacional no prevén limitaciones a la facultad conferida a las autoridades de los Estados Unidos, ni la existencia de garantías para personas que no sean estadounidenses. ² El artículo 702 de la FISA se aplica a todos los “proveedores de servicios de comunicación electrónica” (véase la definición en 50 USC § 1881(b)(4)), mientras que la EO 12 333 organiza la vigilancia electrónica, que se define como la “adquisición de una comunicación no pública por medios electrónicos sin el consentimiento de una persona que sea parte en una comunicación electrónica o, en el caso de una comunicación no electrónica, sin el consentimiento de una persona que esté visiblemente presente en el lugar de la comunicación, pero sin incluir el uso de un equipo de la radio; B)”.

3) ¿Hay algún período de gracia durante el cual pueda seguir transfiriendo datos a los EE.UU. sin evaluar mi base legal para la transferencia?

➔ No, el Tribunal ha invalidado la Decisión sobre el Escudo de Privacidad sin mantener sus efectos, porque la ley estadounidense evaluada por el Tribunal no proporciona un nivel de protección esencialmente equivalente a la UE. Esta evaluación debe tenerse en cuenta para cualquier transferencia a los Estados Unidos.

4) Yo estaba transfiriendo datos a un importador de datos de EE.UU. adherido al Escudo de Privacidad, ¿qué debo hacer ahora?

➔ Las transferencias basadas en este marco jurídico son ilegales. Si desea seguir transfiriendo datos a los EE.UU., tendrá que comprobar si puede hacerlo en las condiciones establecidas a continuación.

5) Estoy usando CCEs con un importador de datos en los EE.UU., ¿qué debo hacer?

➔ El Tribunal de Justicia considera que el derecho de los Estados Unidos (es decir, el artículo 702 de la FISA y la EO 12333) no garantiza un nivel “*esencialmente equivalente*” de protección.

El hecho de que pueda usted o no transferir datos personales sobre la base de los CCEs dependerá del resultado de su evaluación, teniendo en cuenta las circunstancias de las transferencias, y las medidas suplementarias que podría adoptar. Las medidas suplementarias junto con los CCEs, tras un análisis caso por caso de las circunstancias de la transferencia, tendrían que garantizar que la legislación de los Estados Unidos no infrinja el nivel adecuado de protección que garantizan.

Si llega a la conclusión de que, teniendo en cuenta las circunstancias de la transferencia y las posibles medidas suplementarias, no se garantizarían las garantías adecuadas, se le exige que suspenda o ponga fin a la transferencia de datos personales. Sin embargo, si tiene la intención de seguir transfiriendo datos a pesar de esta conclusión, debe notificar a su AS³ competente.

6) Estoy usando normas corporativas vinculantes («NCVs») con una entidad en los EE.UU., ¿qué debo hacer?

➔ Dada la sentencia del Tribunal ha invalidado el Escudo de Privacidad debido al grado de interferencia creado por la ley de los Estados Unidos con los derechos fundamentales de las personas cuyos datos se transfieren a ese tercer país y el hecho de que el Escudo de Privacidad también fue diseñado para dar garantías a los datos transferidos con otros instrumentos como las NCVs (normas corporativas vinculantes), la evaluación del Tribunal se aplica también en el contexto de las NCVs, ya que la legislación estadounidense también tendrá primacía sobre esta herramienta.

El hecho de que pueda usted o no transferir datos personales sobre la base de las NCVs dependerá del resultado de su evaluación, teniendo en cuenta las circunstancias de las transferencias, y las medidas suplementarias que podría adoptar. Estas medidas

³ Véase, en particular, el considerando 145 de la sentencia del Tribunal de Justicia. En relación con los CCE, véase la cláusula 4, letra g), Decisión 2010/87/UE de la Comisión, así como la cláusula 5, letra a), Decisión 2001/497/CE de la Comisión y el anexo II, letra c), Decisión 2004/915/CE de la Comisión.

suplementarias, junto con las NCVs, tras un análisis caso por caso de las circunstancias de la transferencia, tendrían que garantizar que la legislación estadounidense no infrinja el nivel adecuado de protección que garantizan.

Si llega a la conclusión de que, teniendo en cuenta las circunstancias de la transferencia y las posibles medidas suplementarias, no se aseguran las garantías adecuadas, se le exige que suspenda o ponga fin a la transferencia de datos personales. Sin embargo, si tiene la intención de seguir transfiriendo datos a pesar de esta conclusión, debe notificar a su autoridad de supervisión competente (Agencia de Protección de Datos)⁴.

7) ¿Qué hay de otros instrumentos de transferencia en virtud del artículo 46 del RGPD?

➔ El CEPD evaluará las consecuencias de la sentencia sobre instrumentos de transferencia distintos de los CCEs y los NCVs. La sentencia aclara que la norma para las garantías adecuadas en el artículo 46 del RGPD es la de la «*equivalencia esencial*».

Como ha subrayado el Tribunal de Justicia, debe remarcarse que el art. 46 se recoge en el Capítulo V del RGPD y, por ello, debe interpretarse a la luz del art. 44 del mismo Reglamento, que establece que “*todas las disposiciones de este capítulo se aplicarán para asegurar que el nivel de protección de las personas físicas garantizado por el Reglamento no se verá menoscabado*”.

8) ¿Puedo confiar en una de las excepciones del artículo 49 del RGPD para transferir datos a los Estados Unidos?

➔ Todavía es posible transferir datos del EEE a los Estados Unidos sobre la base de las excepciones previstas en el artículo 49 del RGPD, siempre que se apliquen las condiciones establecidas en este artículo. El CEPD se remite a sus directrices sobre esta disposición⁵.

En particular, debe recordarse que cuando las transferencias se basan en el consentimiento del afectado, este debe ser:

- explícito,
- específico para la transferencia de datos o conjunto de transferencias particulares (lo que significa que el exportador de datos debe asegurarse de obtener un consentimiento específico antes de que la transferencia se lleve a cabo incluso después de la recogida de los datos), e
- informado, en particular en cuanto a los posibles riesgos de la transferencia (es decir, el afectado también debe informar de los riesgos específicos derivados del hecho de que sus datos se transferirán a un país que no proporciona una

⁴ Véase, en particular, el considerando 145 de la sentencia del Tribunal de Justicia. En relación con los CCE, véase la cláusula 4, letra g), Decisión 2010/87/UE de la Comisión, así como la cláusula 5, letra a), Decisión 2001/497/CE de la Comisión y el anexo II, letra c), Decisión 2004/915/CE de la Comisión. En relación con los BCR, véanse la sección 6.3 WP256 rev.01 (aprobada por el EDPB), y la sección 6.3 WP257 rev.01 (aprobada por el EDPB).

⁵ Véanse las Directrices del BDE 2/2018 sobre excepciones al artículo 49 del Reglamento 2016/679, adoptado el 25 de mayo de 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, p.3. 6

protección adecuada y que no se aplican salvaguardias adecuadas para la protección de los datos).

Por lo que se refiere a las transferencias necesarias para la ejecución de un contrato entre el afectado y el responsable del tratamiento, debe tenerse en cuenta que los datos personales solo pueden transferirse cuando la transferencia sea ocasional. Habría que determinar caso por caso si las transferencias de datos se determinarían como «*ocasionales*» o «*no ocasionales*». En cualquier caso, esta excepción solo puede invocarse cuando la transferencia sea objetivamente necesaria para la ejecución del contrato.

En relación con las transferencias necesarias por razones importantes de interés público (que deben reconocerse en la legislación de la UE o de los Estados miembros de 6⁶), el CEPD recuerda que el requisito esencial para la aplicabilidad de esta excepción es la constatación de un interés público importante y no la naturaleza de la organización, y que aunque esta excepción no se limita a las transferencias de datos que son «*ocasionales*», esto no significa que las transferencias de datos sobre la base de la importante excepción de interés público puedan llevarse a cabo a cabo en gran escala y de manera sistemática.

9) ¿Puedo seguir utilizando CCEs o NCVs para transferir datos a otro tercer país que no sea Estados Unidos?

➡ El Tribunal ha indicado que, por regla general, las CCE pueden seguir utilizándose para transferir datos a un tercer país, sin embargo, el umbral establecido por el Tribunal para las transferencias a los Estados Unidos se aplica a cualquier tercer país. Lo mismo ocurre con las NCVs.

El Tribunal de Justicia destaca que es responsabilidad del exportador de datos y del importador de datos evaluar si el nivel de protección exigido por la legislación de la UE se respeta en el tercer país de que se trate a fin de determinar si las garantías ofrecidas por los CCEs o los NCVs pueden cumplirse en la práctica. Si este no es el caso, debe evaluar si puede proporcionar medidas complementarias para garantizar un nivel de protección esencialmente equivalente a lo dispuesto en el EEE, y si la legislación del tercer país no afectará a estas medidas suplementarias para evitar su eficacia.

Puede usted ponerse en contacto con su importador de datos para verificar la legislación de su país y colaborar para su evaluación. En caso de que usted o el importador de datos del tercer país determinen que los datos transferidos en virtud de las CCEs o de las NCVs no gozan de un nivel de protección esencialmente equivalente al garantizado en el EEE, debe suspender inmediatamente las transferencias. En caso de que decida no hacerlo, deberá notificar su decisión a su autoridad de supervisión⁷ competente.

➡ Aunque, como subraya el Tribunal de Justicia, es responsabilidad primordial de los exportadores de datos y de los importadores de datos evaluar por sí mismos que la

⁶ Referencias a los “Estados miembros” deben entenderse como referencias a los “Estados EEE”.

⁷ Véase, en particular, el considerando 145 de la sentencia del Tribunal de Justicia. En relación con los CCE, véase la cláusula 4, letra g), Decisión 2010/87/UE de la Comisión, así como la cláusula 5, letra a), Decisión 2001/497/CE de la Comisión y el anexo II, letra c), Decisión 2004/915/CE de la Comisión. En relación con los BCR, véanse la sección 6.3 WP256 rev.01 (aprobada por el EDPB), y la sección 6.3 WP257 rev.01 (aprobada por el EDPB).

legislación del tercer país de destino permite al importador de datos cumplir las cláusulas estándar de protección de datos o las BCR, antes de transferir datos personales a ese tercer país, las autoridades de supervisión también desempeñarán un papel clave a la hora de hacer cumplir el RGPD y de adoptar nuevas decisiones sobre transferencias a terceros países.

Como ha invitado el Tribunal de Justicia, con el fin de evitar decisiones divergentes, el CEPD seguirá trabajando para garantizar la coherencia, en particular en caso de que deban prohibirse las transferencias a terceros países.

10) ¿Qué tipo de medidas suplementarias puedo introducir si estoy utilizando CCE o RCE para transferir datos a terceros países?

➔ Las medidas suplementarias que usted podría prever, en caso necesario, deberían preverse caso por caso, teniendo en cuenta todas las circunstancias de la transferencia y tras la evaluación de la legislación del tercer país, a fin de comprobar si garantiza un nivel adecuado de protección.

El Tribunal de Justicia destacó que es responsabilidad primordial del exportador de datos y del importador de datos efectuar esta evaluación y adoptar las medidas complementarias necesarias.

El CEPD está analizando actualmente la sentencia del Tribunal de Justicia para determinar el tipo de medidas suplementarias que podrían proporcionarse además de los CCE o los RCE, ya sean medidas jurídicas, técnicas u organizativas, para transferir datos a terceros países en los que los CCE o los RCE no proporcionen por sí solos el nivel suficiente de garantías.

➔ El CEPD está estudiando más a fondo en qué podrían consistir estas medidas suplementarias y proporcionará más orientación.

11) Estoy utilizando un encargado que trata datos de los que soy responsable, ¿cómo puedo saber si este encargado transfiere datos a los EE.UU. o a otro tercer país?

➔ El contrato que ha celebrado con su encargado de conformidad con el artículo 28.3 del RGPD debe indicar si las transferencias están autorizadas o no (debe tenerse en cuenta que incluso proporcionar acceso a datos de un tercer país, para fines administrativos, por ejemplo, también equivale a una transferencia).

➔ También debe concederse autorización a los encargados para que estos encomienden a los subencargados la transferencia de datos a terceros países. Debe usted prestar atención y tener cuidado, ya que una gran variedad de soluciones informáticas puede implicar la transferencia de datos personales a un tercer país (por ejemplo, para fines de almacenamiento o mantenimiento).

12) Que puedo hacer para continuar utilizando los servicios de mi encargado si el contrato firmado con arreglo al art. 28.3 del RGPD establece que los datos pueden transferirse a los EE.UU. o a cualquier otro tercer Estado.

➔ Si sus datos pueden transferirse a los EE.UU. y no se pueden proporcionar medidas suplementarias para garantizar que la legislación estadounidense no afecte al nivel de protección esencialmente equivalente que ofrecen los instrumentos de transferencia en el EEE, ni cabe aplicar alguna de las excepciones en virtud del artículo 49 del RGPD, la única solución es negociar una enmienda o cláusula suplementaria de su contrato para

prohibir las transferencias a los EE.UU. Los datos no solo deben almacenarse sino también administrarse en otro lugar que en los EE.UU.

➔ Si sus datos pueden transferirse a otro tercer país, también debe usted verificar la legislación de ese tercer país para comprobar si cumplen los requisitos del Tribunal y el nivel de protección de los datos personales esperado. Si no encuentra ninguna finalidad adecuada para las transferencias a un tercer país, los datos personales no deben transferirse fuera del territorio del EEE y todas las actividades de tratamiento deben llevarse a cabo en el EEE.

Por el Comité Europeo de Protección de Datos

La Presidencia

Andrea Jelinek