IMPLICACIONES DE LA DECLARACIÓN DE INVALIDEZ DEL ESCUDO DE PRIVACIDAD

Pedro Alberto DE MIGUEL ASENSIO *

Publicado en:

La Ley Unión Europea,

Número 84, septiembre 2020, pp. 1-5

ISSN 2255-551X

* Catedrático de Derecho internacional privado
Facultad de Derecho
Universidad Complutense de Madrid
E- 28040 MADRID
pdmigue@ucm.es

Implicaciones de la declaración de invalidez del Escudo de Privacidad

Pedro Alberto de Miguel Asensio
Catedrático de Derecho internacional privado
Universidad Complutense de Madrid

SUMARIO: La declaración de invalidez por el Tribunal de Justicia de la Decisión de la Comisión sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EEUU priva de eficacia a una vía fundamental para facilitar las transferencias de datos personales desde la UE a EEUU. El fundamento de esa declaración de invalidez y las consecuencias que extrae de las carencias en el potencial acceso a datos personales con fines de seguridad pública por parte de las autoridades de EEUU tendrán importantes implicaciones de cara al futuro, tanto en el diseño y aplicación de las decisiones de adecuación con base en el artículo 45 RGPD, como en relación con el ofrecimiento, como alternativa, de garantías adecuadas en virtud del artículo 46, con base en cláusulas tipo de protección de datos. Incluso cabe prever también repercusiones en la aplicación de otras garantías, como las resultantes de normas corporativas vinculantes, e incluso en la aplicación de la excepción basada en el consentimiento explícito a la transferencia por parte del interesado.

PALABRAS CLAVE: datos personales, transferencias, Escudo de Privacidad, cláusulas tipo de protección de datos

ABSTRACT: The declaration of invalidity by the Court of Justice of the Commission Decision on the adequacy of the protection provided by the EU-US Privacy Shield deprives of effectiveness a basic mechanism to facilitate the transfer of personal data from the EU to the US. The rationale for such a declaration of invalidity and the consequences it draws from the shortcomings in the potential access to personal data for public security purposes by the US authorities will have important implications for the future. Such consequences will affect the design and implementation of adequacy decisions based on Article 45 GDPR and the provision, as an alternative, of appropriate safeguards under Article 46, in particular, recourse to standard data protection clauses. An impact on the application of other safeguards, such as those resulting from binding corporate rules, and even on the application of the exception based on the explicit consent to the proposed transfer by the data subject can also be foreseen.

KEYWORDS: personal data, transfers, Privacy Shield, standard data protection clauses

I. Introducción

Elemento fundamental de la sentencia del Tribunal de Justicia de 16 de julio de 2020 en el asunto *Facebook Ireland y Schrems*, C-311/18, EU:C:2020:559, es la declaración de invalidez de la Decisión de Ejecución (UE) 2016/1250 de la Comisión sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-

EEUU. Hasta esa declaración el llamado Escudo de Privacidad servía de fundamento legal a una parte muy significativa de las transferencias de datos personales desde la UE hasta EEUU, en la medida en que estuvieran destinadas a entidades establecidas en EEUU adheridas al Escudo de privacidad. La trascendencia práctica de la declaración de invalidez se ve acentuada por el pronunciamiento del Tribunal de Justicia de no mantener los efectos de la mencionada Decisión de Ejecución (UE) 2016/1250, por considerar que su anulación no crea un vacío legal, habida cuenta de que el régimen aplicable a las transferencias de datos entre la UE y EEUU viene determinado, en ausencia de una decisión de adecuación –como la que establecía el Escudo de Privacidad y que resulta invalidada-, por lo dispuesto básicamente en el artículo 49 RGPD (apdo. 202 de la sentencia). Más allá de las consecuencias derivadas de la anulación del Escudo de Privacidad y la imposibilidad de realizar transferencias a EEUU sin necesidad de autorización con base en esa decisión de adecuación conforme al artículo 45 RGPD, el fundamento de la sentencia *Facebook Ireland y Schrems* para declarar la invalidez tiene también implicaciones muy significativas en relación con las posibles alternativas para transferir datos a EEUU (y otros terceros Estados) en virtud del Capítulo V del RGPD.

II. Fundamento de la declaración de invalidez de la Decisión de la Comisión sobre el Escudo de Privacidad

La anulación de la Decisión sobre el Escudo de Privacidad es consecuencia de la apreciación por el Tribunal de Justicia de que la constatación por la Comisión en esa Decisión de que EEUU garantiza efectivamente un nivel de protección adecuado –es decir, sustancialmente equivalente al que asegura el ordenamiento jurídico de la Unión- de los datos personales transferidos en virtud del Escudo de Privacidad no se corresponde con la realidad. Básicamente los derechos fundamentales implicados son los garantizados en los artículos 7 y 8 de la Carta. El primero recoge el derecho al respeto a la vida privada y familiar, de su domicilio y de sus comunicaciones, mientras que el artículo 8.1 reconoce a toda persona el derecho a la protección de los datos de carácter personal que le conciernan. Pero también resultan relevantes otros, especialmente el derecho fundamental a la tutela judicial efectiva del artículo 47 de la Carta.

En concreto, el Tribunal de Justicia constata que la Decisión sobre el Escudo de Privacidad admite con carácter general posibles injerencias de las autoridades de EEUU en los derechos fundamentales de los afectados cuyos datos son objeto de transferencia que puedan resultar de exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de EEUU. La principal preocupación a este respecto deriva de la eventual utilización de esos datos por las autoridades estadounidenses a esos efectos en el marco de programas de vigilancia de sus servicios de inteligencia, como los sistemas de vigilancia PRISM o Upstream, que no se encuentran sujetos a exigencias que aseguren el respeto del principio de proporcionalidad en el alcance de esas injerencias, ya que no se ciñen a lo estrictamente necesario. El Tribunal pone de

relieve la falta de limitaciones en lo relativo a la ejecución de esos programas de vigilancia –que, por ejemplo, permiten la recopilación en bloque de datos personales en tránsito hacia EEUU sin ningún control judicial-, la ausencia de garantías para las personas no nacionales de los EEUU que sean objeto de tales programas, así como la no atribución a esos interesados de derechos exigibles a las autoridades estadounidenses ante los tribunales (apdos. 180-185 de la sentencia de 16 de julio de 2020).

El segundo ámbito en la que el Tribunal de Justicia constata que la situación en EEUU no permite garantizar un nivel de protección sustancialmente equivalente al garantizado en el ordenamiento jurídico de la Unión es el relativo a la exigencia de un control jurisdiccional efectivo, proclamado por el artículo 47 de la Carta y que reclama posibilidades efectivas de que el interesado ejercite acciones administrativas y judiciales en el país tercero destino de la transferencia de sus datos personales. El Tribunal pone de relieve que las lagunas existentes a este respecto en el ordenamiento de EEUU –en especial, la inexistencia en el marco de los programas de vigilancia de derechos de los interesados exigibles a las autoridades de EEUU ante los tribunales- no son subsanadas mediante la creación en marco del Escudo de Privacidad de la figura del mecanismo específico del Defensor del Pueblo establecido a estos efectos por las autoridades de EEUU. Ese singular mecanismo no garantiza que los interesados tengan la posibilidad de ejercer acciones ante un tribunal independiente e imparcial para acceder a los datos personales que les conciernen o para obtener su rectificación o supresión (apdos. 194 a 198 de la sentencia).

III. Tratamiento de datos personales con fines de seguridad nacional

En la medida en que las prácticas de EEUU cuya compatibilidad con la garantía de un nivel de protección adecuado se cuestionaba resultaban básicamente del eventual tratamiento de los datos transferidos por las autoridades de ese país por razones de seguridad nacional y a efectos de la aplicación de la ley y de la administración de los asuntos exteriores del país, la primera de las cuestiones prejudiciales planteadas buscaba respuesta a las dudas que podían surgir con respecto a la eventual aplicación de la legislación sobre datos personales de la Unión a estas situaciones. Conforme al artículo 4.2 del Tratado de la Unión Europea, la Unión respeta las funciones esenciales del Estado, como mantener el orden público y salvaguardar la seguridad nacional, especificando que la seguridad nacional seguirá siendo responsabilidad exclusiva de cada Estado miembro. Por su parte, el artículo 2.2 RGPD establece que el Reglamento no se aplica al tratamiento de datos personales en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión (apdo a); al tratamiento por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de la Política Exterior y de Seguridad Común (apdo. b); ni al tratamiento 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 (apdo d).

El Tribunal de Justicia considera que ninguna de estas exclusiones resulta relevante a los efectos de que el Derecho de la Unión en materia de protección de datos personales no sea aplicable con respecto a transferencias de datos personales entre dos operadores económicos con fines comerciales, en el caso del litigio principal Facebook Ireland y Facebook Inc. Una vez constatado que el Derecho de la Unión en materia de protección de datos personales es aplicable en todo caso a ese tipo de transferencias, el Tribunal considera que eso necesariamente debe incluir el eventual control de los ulteriores tratamientos a que esos datos personales se puedan ver expuestos como consecuencia de su transferencia aunque tengan lugar con fines de seguridad pública, defensa o seguridad del Estado por parte de las autoridades del país tercero de que se trate (apdos. 86 y 87 de la sentencia).

Más allá del caso concreto, este planteamiento del Tribunal de Justicia será relevante a efectos de futuras decisiones de adecuación respecto de Estados terceros condicionando la evaluación de la Comisión contemplada en el artículo 45.3, que habrá de prestar especial atención a los ulteriores tratamientos a los que puedan verse sometidos los datos transferidos por las autoridades del tercer Estado con fines de seguridad pública. Ciertamente, esta constatación puede condicionar futuras decisiones de adecuación, por ejemplo, en relación con el Reino Unido en el marco del Brexit, e incluso requerir la revisión de alguna de las ya adoptadas, en la medida en que puedan surgir dudas sobre este particular. A este respecto, resulta relevante la doctrina del Tribunal de Justicia según la cual las decisiones de la Comisión sobre adecuación tienen carácter obligatorio para las autoridades de control nacionales, que no pueden suspender o prohibir transferencias comprendidas en una de esas decisiones mientras no sea declarada inválida por el Tribunal de Justicia. Ahora bien, en caso de que un interesado cuyos datos sean objeto de transferencia ponga en entredicho fundadamente el que las transferencias basadas en una de esas decisiones cumplen con las exigencias establecidas por el RGPD, la autoridad de control debe interponer un recurso ante los tribunales nacionales para que estos planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de esa decisión (apdos. 156 a 158 de la sentencia).

IV. Transferencias mediante cláusulas tipo de protección de datos y otras garantías adecuadas

Como es sabido, en la medida en que con respecto al tercer Estado destino de la transferencia de datos personales no exista una decisión de adecuación en virtud del artículo 45 RGPD, las transferencias solo pueden realizarse si existen garantías adecuadas conforme a lo previsto en el artículo 46.2 RGPD o, en su defecto, cuando sea aplicable alguna de las excepciones para situaciones específicas establecidas en el artículo 49 RGPD.

Con respecto a las garantías adecuadas, la sentencia de 16 de julio en el asunto C-311/18 dedica atención detallada al empleo de cláusulas tipo de protección de datos (art. 46.2.c) RGPD), habida cuenta de que Facebook Ireland había puesto de relieve su

empleo como fundamento de las transferencias cuestionadas. Si bien el Tribunal de Justicia confirma la validez de la Decisión de la Comisión 2010/87/UE relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, en su versión modificada por la Decisión de Ejecución (UE) 2016/2297, lo cierto es que la sentencia está llamada a tener una profunda repercusión sobre el uso de este tipo de garantías como fundamento de transferencias a terceros Estados, en particular en las relaciones transatlánticas.

Tanto para el uso de esas cláusulas tipo como para el empleo de otras garantías adecuadas tendrá especial repercusión en el futuro las consecuencias que el Tribunal extrae de la exigencia de asegurar que las personas cuyos datos personales son objeto de transferencia a un país tercero con base en una de esas garantías gozan respecto de los datos transferidos de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión (apdo. 96 de la sentencia). En la medida en que las carencias de la normativa del tercer Estado destinatario de los datos, por ejemplo, en lo relativo al ulterior acceso de las autoridades de ese país a los datos transferidos, puedan tener como consecuencia que el empleo de las cláusulas tipo entre las partes de la transferencia no resulta suficiente para asegurar un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión, la transferencia no estará amparada con base en el artículo 46.2 RGPD. De hecho, en tales situaciones, la autoridad nacional de control estará obligada a suspender o prohibir la transferencia de datos personales (apdo. 113 de la sentencia).

Por consiguiente, el empleo de cláusulas tipo no exime de la necesidad de valorar si, a la luz de las circunstancias que rodean la transferencia, las cláusulas tipo de protección de datos no se respetan o no pueden ser respetadas en el país tercero al que los datos van a ser transferidos, de modo que no puede garantizarse un nivel de protección equivalente al existente en la UE. En relación con las transferencias entre la UE y EEUU, las carencias en el sistema jurídico estadounidense que sirven de fundamento en la sentencia a la declaración de invalidez de la Decisión de la Comisión sobre el Escudo de Privacidad, parecen poner también en entredicho el que la transferencia pueda tener lugar de modo respetuoso con lo exigido en el RGPD mediante el empleo de cláusulas tipo de protección. Incluso aunque la sentencia no aborda esta cuestión es de prever que se planteen dudas similares con respecto al empleo de otras garantías contempladas en el artículo 46, como es el caso de las normas corporativas vinculantes, en las transferencias entre la UE y EEUU.

V. Excepciones para situaciones específicas: el consentimiento explícito del interesado

En defecto de decisión sobre adecuación y de garantías adecuadas, las transferencias únicamente son posibles si concurre alguna de las excepciones para situaciones específicas establecidas en el artículo 49 RGPD. Al margen de que la transferencia resulte necesaria para determinadas finalidades (como la ejecución de un

contrato), tiene especial importancia práctica la posibilidad de que el interesado haya dado explícitamente su consentimiento a la transferencia (art. 49.1.a) RGPD). De hecho, en el asunto C-311/18 el Gobierno alemán consideraba que las cuestiones prejudiciales eran inadmisibles por no haber comprobado el órgano de remisión si el interesado cuyos datos eran objeto de transferencia había dado su consentimiento de forma indubitada a las transferencias, lo que tendría como efecto hacer innecesaria una respuesta a esa cuestión (apdo. 72). No obstante, el Tribunal constató que Facebook Ireland había reconocido que una gran parte de sus transferencias de datos personales a Facebook Inc. cuya legalidad se impugnaba, se realizaban sobre la base de cláusulas tipo de protección de datos (apdo. 74).

Aunque no aborde esta cuestión, cabe considerar que más allá de lo ya señalado, la nueva sentencia también condicionará el eventual recurso a la excepción basada en el consentimiento del interesado como fundamento de las transferencias a EEUU. En concreto, el artículo 49.1.a) RGPD no solo exige que el consentimiento a la transferencia propuesta haya sido otorgado por el interesado de manera explícita sino que requiere además que tal consentimiento se preste por el interesado "tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas".

VI. Reflexión final

Mucho se ha escrito en los últimos años acerca del RGPD y su importancia como reflejo del potencial de la UE para difundir los valores en los que se funda en otras regiones del mundo, habida cuenta de la influencia clave de la legislación de protección de datos personales de la UE en la elevación de los estándares de protección en la materia en muchos países del mundo. Esta sentencia además de contribuir a perfilar el alcance de la protección de datos personales en la UE y salvaguardar su eficacia en lo relativo a las transferencias internacionales pone una vez más de relieve la deficiente aplicación de la legislación de la Unión en la materia. Así resulta de que pese al poder de las autoridades nacionales de control (y de la Comisión para no adoptar una Decisión como la ahora declarada inválida especialmente tras la experiencia anterior del sistema de Puerto Seguro), sea la reclamación de un particular la que lleve a constatar con evidente retraso la "ilegalidad" de innumerables transferencias de datos de millones de interesados de la Unión Europea. Por ello, esta sentencia debe también mover a la reflexión acerca del coste para la Unión Europea de la deficiente aplicación a operadores situados en terceros Estados del marco europea, en especial ante la evidencia de la ausencia de operadores globales de origen europeo en sectores como las redes sociales o los motores de búsqueda. No se trata de una crítica al elevado nivel de protección del que se ha dotado la Unión Europea sino a su deficiente aplicación práctica en el contexto de globalización de la actividad empresarial característico del entorno digital.