REVISTA LEX MERCATORIA
ISSN 2445-0936

Vol. 17, 2021. Artículo 4
DOI: 10.21134/lex.vi17.1415

SENTENCIA SCHREMS II: LOCALIZACIÓN DE DATOS PERSONALES Y SU IMPACTO EN LOS SERVICIOS DIGITALES

Javier López Guzmán
Analista jurídico y doctorando
Universidad Libre de Bruselas (Bélgica-VUB)

Javier López Guzmán

Resumen

La sentencia del caso Schrems II ha sacudido la economía digital. Se ha convertido en uno de los hitos en la regulación de la privacidad desde que el Reglamento General de Protección de Datos fue aprobado en la Unión Europea. Se analiza aquí el recurrido de la serie judicial y sus consecuencias en la transferencia internacional de datos personales y su impacto en los servicios digitales.

Abstract

The Schrems II judgment has shaped digital economy in an unprecedented way. It has become one of the milestones in privacy regulation since the creation in the European Union of the General Data Protection Regulation. This article analyses the Schrems series and the consequences in the international personal data transfers and its impact in digital services.

Lista de palabras clave

Protección de datos personales. Privacidad. Transferencias Internacionales de Datos Personales. Schrems. Escudo de Privacidad. Cláusulas Contractuales Tipo. Decisión de adecuación.

Keywords

Data protection. Privacy. Internacional Personal Data Transfers. Schrems. Privacy Shield. Standard Contractual Clauses. Adequacy Decisions.

Sumario

El 16 de julio de 2020, el Tribunal de Justicia de la Unión Europea dictó una sentencia que marca un hito en el ámbito de la protección de datos personales y la sociedad de la información. El caso Schrems II[1] trasciende estas áreas de conocimiento y tiene una enorme repercusión en el mercado digital, a nivel de la UE, y a nivel mundial. Y, por tanto, en la vida de millones de ciudadanos, usuarios de redes sociales y servicios digitales en todo el mundo. Este impacto se analizará con más detalle en este artículo. Si le interesa el tema, siga leyendo. Pero tenga en cuenta que el derecho es como las salchichas. Si le gustan, quizá sea mejor no averiguar cómo se hacen.

Esta sentencia (¿tal vez?) pone fin a la serie Schrems. Maximilian Schrems, ciudadano austriaco, comenzó a desafiar el régimen de gestión internacional de datos personales de las redes sociales en 2013. Tras las revelaciones de Snowden, el mundo se dio cuenta de que muchos de los servicios digitales utilizados a nivel global eran una fuente de información personal al alcance de cualquier gobierno interesado en ella. Pero especialmente al alcance de la administración de los Estados Unidos de América y sus programas de vigilancia masiva. Estas revelaciones inspiraron muchas acciones en defensa de los derechos fundamentales, la privacidad y la protección de los datos personales. El Sr. Schrems eligió el campo de batalla de las redes sociales. Así, desafió el régimen de gestión de datos de la mayor red social del momento: Facebook.

I. Schrems I.

Maximilian Schrems presentó varias denuncias contra Facebook ante el Comisario de Protección de Datos de Irlanda ("DPC"), basándose, entre otros motivos, en la pertenencia de Facebook al Puerto Seguro UE-EE.UU. y sus obligaciones. ¿Por qué en Irlanda? La empresa, como muchos otros actores digitales globales, tiene su sucursal europea con sede allí por motivos regulatorios y fiscales, Facebook Ireland, Ltd; que es responsable del tratamiento de los datos personales de sus usuarios en Europa. ¿Y por qué el Puerto Seguro? Esta estructura legal fue creada por la Unión Europea y Estados Unidos para cubrir la legalidad de las transferencias internacionales de datos personales a Estados Unidos. Siguiendo este esquema, las empresas tecnológicas que quisieran obtener datos personales de usuarios europeos y tratarlos en EEUU podrían hacerlo. Tendrían que seguir una serie de requisitos, pero estas transferencias estaban permitidas ya que la Unión Europea consideraba que la protección de los datos personales en EE.UU. era "sustancialmente equivalente" a la otorgada por la normativa europea. (según el artículo 45 del RGPD).[2]

Esta batalla legal comenzó en 2013, con esta impugnación de las transferencias internacionales de datos personales ante los tribunales irlande-

1 Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 16 de julio de 2020, En el asunto C-311/18, entre Data Protection Commissioner y Facebook Ireland Ltd, Maximillian Schrems. Disponible en: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=es&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=es&avg=&cid=5304939

2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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.

ses, que finalmente llegó al Tribunal de Justicia Europeo. Los demandantes consideraban que este plan eludía la aplicación del RGPD y hacía que los ciudadanos europeos fueran vulnerables a los programas de vigilancia masiva de la administración estadounidense. Por lo tanto, EE.UU. se había convertido de facto en un tercer país no adecuado para la transferencia de los datos personales. Dado que esta decisión se adoptó a raíz de una competencia europea en virtud de la legislación de la UE, los tribunales irlandeses tuvieron que plantear una cuestión prejudicial al TJUE sobre la interpretación de las leyes europeas para el caso (artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea[3] y artículos 25(6) y 28 de la Directiva 95/46/CE, la Directiva de Protección de Datos)[4] y la validez del Puerto Seguro. En octubre de 2015, el TJUE[5] dictaminó que el Puerto Seguro era nulo, debido a que limitaba los poderes de investigación de las autoridades nacionales de protección de datos de los Estados miembros, y a otra serie de razones. Se podría pensar que con esto podría haber terminado el asunto y que los actores del pleito se darían por vencidos. Para nada.

El data mining o extracción de datos personales es demasiado importante en nuestra industria digital actual. Ya era demasiado importante en 2016 para dejar simplemente que el flujo de datos se detuviera. A todos los actores del ámbito digital les interesaba continuar con estas transferencias (industria, gobierno de Estados Unidos y Estados miembros de la UE). A pesar de los reconocidos y continuos ataques a los derechos fundamentales. En consecuencia, se aprobó una nueva decisión de adecuación. El Escudo de Privacidad[6] sustituyó al anulado Puerto Seguro. Este nuevo régimen de transferencia de datos introdujo cambios tras la sentencia Schrems I. Sin embargo, no solucionaba el problema del acceso a estos datos personales por parte de la administración estadounidense para sus programas de vigilancia masiva.

II. Schrems II.

El Escudo de Privacidad fue impugnado en diciembre de 2015, una vez más, por el Sr. Schrems, llevando el caso ante los tribunales irlandeses, que terminó de nuevo ante el TJUE, dictando la sentencia de este pasado verano. El Escudo de Privacidad introdujo cambios, pero los problemas fundamentales de protección de datos personales y el choque con el RGPD se mantuvieron. Facebook y el regulador irlandés trataron de agitar el debate argumentando que el Escudo de Privacidad no era el único paraguas legal válido para sus actividades. Se pusieron sobre la mesa otros instrumentos legales reconocidos en el RGPD: Las Cláusulas Contractuales Tipo y las Normas Corporativas Vinculantes. Estos documentos han sido objeto de estudio y tienen una gran impor-

3 Carta de los Derechos Fundamentales de la Unión Europea 2012/C 326/02.

4 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.

5 Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala) de 6 de octubre de 2015 (petición de decisión prejudicial planteada por la High Court — Irlanda) — Maximillian Schrems / Data Protection Commissioner (Asunto C-362/14)

6 Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE. UU.

tancia en la actualidad, ya que son la operación válida para realizar transferencias cuando el país receptor no tiene una decisión de adecuación reconocida por la UE.

Una vez más, el Tribunal europeo se mostró a favor de los argumentos esgrimidos por los recurrentes y declaró inválido el Escudo de Privacidad. La base de la sentencia es la interpretación que hace el Tribunal de los artículos 46(1), 46(2)(c) y 58(2)(f), (j) del RGPD. Si una Autoridad nacional de control independiente de protección de datos (por ejemplo, la CPD irlandesa) considera que una transferencia de datos personales a un tercer país no garantiza los derechos fundamentales de los interesados europeos, debe ordenarse su suspensión. Independientemente de la presencia o no de una decisión de adecuación en vigor con ese país. El Escudo de Privacidad no es válido, porque considera adecuada la estructura jurídica de EEUU para el tratamiento de los datos personales de los ciudadanos europeos, sin proporcionar recursos administrativos y judiciales para este tratamiento. Si un ciudadano estadounidense quiere impugnar estos programas de vigilancia masiva o impugnar el uso indebido de sus datos personales por motivos policiales, está protegido por las enmiendas de la Constitución de Estados Unidos. Pero un ciudadano europeo no puede impugnar este tratamiento. Ni ante la Administración estadounidense ni ante los tribunales de ese país. Esto no está en consonancia con los derechos fundamentales reconocidos en la Carta de la UE y la protección de datos personales del RGPD.

III. Próximamente.

El Tribunal ha anulado el principal instrumento legal para operar las transferencias a los Estados Unidos. Pero ha mantenido la validez del uso de las SCC y las BCR con garantías adicionales. Esto sigue siendo una vía para que los grandes responsables del tratamiento de datos saquen los datos personales de la Unión. Aunque en el futuro también será problemática para los grandes operadores tecnológicos. El uso de estas cláusulas aún debe ser controlado por las autoridades de protección de datos. Si el tercer país al que se exportan los datos personales no ofrece una protección esencialmente equivalente a la del RGPD, no importa el instrumento jurídico que haya detrás.

Esto es lo que el CPD irlandés se ha visto obligado a decidir tras Schrems II. Actualmente se están celebrando audiencias en el Tribunal Supremo irlandés para decidir si Facebook puede seguir utilizando las SCC para transferir datos a Estados Unidos. Pero este caso no se refiere únicamente a Facebook. Muchos otros grandes actores tecnológicos se apoyan ahora en este instrumento. Y la mayoría (si no todas) de las empresas que crean servicios que utilizamos a diario envían nuestros datos personales fuera de la UE. Las redes sociales, los servicios de almacenamiento en la nube, los servicios de correo electrónico, los sistemas operativos de nuestros dispositivos digitales, los servicios de videollamadas y muchos otros proveedores de servicios digitales. Lo hacen porque el tratamiento de estos datos en conjunto es muy rentable. Y a la Administración estadounidense también le interesa proteger la posición dominante de sus empresas en el mercado global. Facebook ha cuestionado la continuidad de sus servicios en Europa si se detienen los flujos de datos personales.

La importancia de la sentencia Schrems II está en el propio proceso legislativo de la Unión Europea, pero también en la industria digital y la geopolítica. La sentencia afecta al tratamiento, extracción y uso para la vigilancia masiva de los datos personales de los ciudadanos de la UE.

Siendo la UE la vanguardia actual en materia de privacidad digital, afecta indirectamente a todos los ciudadanos y usuarios digitales del mundo. En un futuro próximo, las ONG y las asociaciones de interés público en defensa de los derechos sociales tendrán un papel importante que desempeñar. Numerosas acciones contra estas prácticas fueron presentadas ante los tribunales por organizaciones como NOYB (fundada por Max Schrems tras la serie judicial) y La Quadrature du Net en Europa, y EPIC en Estados Unidos.

IV. Consecuencias de la sentencia.

La sentencia Schrems II ha tenido un importante impacto en la industria, para los usuarios individuales y para las pequeñas y medianas empresas. Marcará las relaciones internacionales en los próximos meses y tendrá un efecto en la relación entre la UE y los Estados Unidos. La administración de Biden en EE.UU. ha sido vista como una esperanza para la recuperación de la confianza en el comercio internacional y un impulso para la relación transatlántica. Pero esto no significa que la nueva administración se alinee con las prioridades de la UE en materia de protección de datos personales. La nueva administración estadounidense está más bien orientada a la industria. Y el centro de atención en las relaciones internacionales ya no es el Atlántico. Es el Pacífico y la relación y rivalidad económica con China.

Todo esto no significa que no haya espacio para acordar y mejorar las normas de protección de datos. Algunos estados de EE.UU. ya han empezado a desarrollar leyes a favor de la privacidad y a limitar las prácticas de la industria y el gobierno. Una decisión de adecuación en la UE para estos estados individuales, además de los EEUU como bloque, es una posibilidad que estaba en la mente de los altos funcionarios de la UE.

La tendencia actual en Europa, sin embargo, está dominada por otras prioridades. En un mundo en el que los datos son el combustible de la economía, conceptos como la localización y la soberanía de los datos son cada vez más importantes. La Autoridad nacional francesa (CNIL) hizo un llamamiento para no almacenar datos sensibles, como los de salud, en servicios en la nube fuera de la UE. Las autoridades de protección de datos a nivel europeo, por su parte, se han centrado en desarrollar las consecuencias de la sentencia. La sentencia también ha tenido un impacto en el Brexit, siendo el Reino Unido un importante receptor de transferencias de datos del resto del bloque de la UE. Y también miembro de la alianza de la vigilancia de los 5 eyes y un agente activo en la pelea por los derechos fundamentales en este sentido.

El Comité Europeo de Protección de Datos ha publicado dos documentos importantes a este respecto: Las Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE y las Recomendaciones 02/2020 sobre las garantías esenciales europeas para medidas de vigilancia. La Comisión Europea, por su parte, ha lanzado una propuesta sobre nuevas Cláusulas Contractuales Tipo. Se hicieron para despejar el camino a los responsables del tratamiento y ayudarles a orientarse en un juicio difícil y técnico, que ha dejado en el limbo a gran parte de nuestro sistema de información. En la actualidad han pasado una serie de consultas a nivel interno en la Comisión Europea y los organismos de protección de datos a nivel comunitario. Se prevé que en el futuro próximo se presenten para su aprobación a través del procedimiento de comitología de la Unión.

Estas medidas y la negociación prevista entre la UE y EE.UU. tras la sentencia ya han sido criticadas por activistas y académicos. Max Schrems lo resumió con bastante precisión en esta declaración: "No hay ninguna "medida complementaria" que se pueda poner en un papel para que una empresa estadounidense que tiene acceso de hecho a los datos ignore la #FISA702 - la única "medida complementaria" que puede arreglar eso está en manos del legislador estadounidense".

La evolución de los servicios digitales y las transferencias internacionales de datos personales en el futuro sigue siendo imprevisible. Es seguro que seguirán teniendo un impacto en el mercado digital y en los derechos fundamentales en Europa y en todo el mundo. Permaneceremos atentos y estudiaremos estas consecuencias.