LAS TRANSFERENCIAS DE DATOS A EE.UU.: LA TRANSICIÓN DEL *SAFE HARBOR* AL *PRIVACY SHIELD* Y UN PASO MÁS ALLÁ

Leticia López Lapuente
*Abogada**

Las transferencias de datos a EE. UU.: la transición del *Safe Harbor* al *Privacy Shield* y un paso más allá

Los flujos de datos entre la Unión Europea y EE. UU. son cruciales para el desarrollo de la economía. La existencia de un marco jurídico estable que habilite dichos flujos garantizando el respeto a los derechos y libertades de los ciudadanos europeos deviene, por tanto, en algo esencial. El marco jurídico actual, el acuerdo de Privacy Shield, se enfrenta a algunos retos que deben resolverse para evitar que se produzca una nueva etapa de inseguridad jurídica como la vivida tras la sentencia en el caso Schrems.

Data transfers to the US: from Safe Harbor to Privacy Shield and one step further

The data flows between the European Union and the US are crucial for the development of our economies. The existence of a stable legal framework enabling such data flows, while ensuring the protection of the rights and freedoms of the European citizen become an essential matter. The current legal framework, i.e., the Privacy Shield, faces certain challenges that need to be solved in order to avoid a new period of legal uncertainty such as the one following the Schrems ruling.

Palabras clave
Escudo de privacidad, Transferencias de datos, Protección de datos, Sentencia Schrems y Puerto seguro.

Key words
Privacy Shiel', Data transfers, Data protection, Schrems case y Safe Harbor.

Fecha de recepción: 30-1-2017 *Fecha de aceptación: 15-2-2017*

En octubre del año 2015, la sentencia del Tribunal de Justicia de la Unión Europea en el caso Schrems[1] dinamitó el principal marco jurídico que, hasta esa fecha, facultaba a las empresas y organizaciones de la Unión Europea a realizar transferencias de datos personales a EE.UU. La sentencia, que declaró la invalidez de la Decisión de la Comisión del año 2000 por la que se aprobaba el acuerdo UE-EE.UU. de *Safe Harbor*[2] (conocido en castellano como «Puerto Seguro») hizo que las entidades estadounidenses adheridas al sistema de *Safe Harbor* perdieran abruptamente su condición de entidad «adecuada» para recibir datos personales de la Unión Europea. Tal como se detalla en la sentencia, las revelaciones hechas públicas en el caso Snowden dejaron al descubierto programas de acceso masivo desde EE.UU. a datos de ciudadanos europeos que resultaban incompatibles con el derecho a la protección de datos de estos. De esta forma, de un día para otro, la mayor parte del tejido empresarial europeo se encontró en una situación de incertidumbre y de riesgo regulatorio, sin causa legítima que amparara sus transferencias internacionales.

Lejos de poder interrumpir sus operaciones con EE.UU. y sin capacidad de modificar de forma fácil y expeditiva sus sistemas de tecnológicos y de información (muchos de ellos soportados por esas entidades estadounidenses de «puerto seguro»), la entidades europeas afectadas por la invalidez del *Safe Harbor* vivieron meses de inseguridad jurídica que —es justo decir— era inmerecida. Amparadas por la legalidad que les otorgaba la Decisión de la Comisión de 2000, incontables empresas y organizaciones europeas, incluidas las españolas, habían adoptado decisiones empresariales lícitas y organizaron sus actividades, contrataron servicios y diseñaron la arquitectura e infraestructura de sus sistemas tecnológicos contando con empresas que ostentaban la condición de puerto seguro. Revertir esas decisiones organizativas o rediseñar sus sistemas eran decisiones de difícil y lenta ejecución y de altísimo coste en numerosas ocasiones. Por ello, durante los meses que siguieron a la declaración de invalidez del sistema de *Safe Harbor*, miles de empresas europeas se lanzaron a la búsqueda de mecanismos jurídicos que hicieran lícitas sus trans-

* Del Área de Derecho Mercantil de Uría Menéndez (Madrid).

1 Sentencia del Tribunal de Justicia de la Unión Europea en el asunto C- 362/14, Maximiliam Schrems vs. Data Protection Comissioner, de 6 de octubre de 2015.

2 Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

ferencias con EE.UU. o que mitigaran sus riesgos de incumplimiento de la normativa de protección de datos en la medida de lo posible. Así, se vio cómo las más de 4.000 empresas estadounidenses que se habían adherido a los principios del *Safe Habor* pasaron a ofrecer a las empresas europeas mecanismos jurídicos alternativos, como son la firma de las Cláusulas contractuales tipo de la Unión Europea o las Reglas corporativas vinculantes. Estas soluciones, razonablemente fáciles de ejecutar en determinadas jurisdicciones de la Unión Europea en las que la firma de estos mecanismos contractuales puede bastar para legitimar transferencias a los EE.UU., no resultan por el contrario un mecanismo ágil en otras jurisdicciones, como España, en las que la firma de estos documentos debe acompañarse de determinadas formalidad y de la obtención de una autorización de autoridad competente (*i. e.*, la Agencia Española de Protección de Datos en el caso de España). Baste señalar, además, que el incumplimiento de las reglas aplicables a las transferencias internacionales de datos tiene la consideración en España de infracción muy grave y podía resultar sancionable con multas de hasta 600.000 euros.

Lo que quedó patente en los meses posteriores a la sentencia Schrems es que la única solución a la invalidez del sistema de *Safe Harbor* como marco habilitador de transferencias transoceánicas UE-EE.UU. pasaba necesariamente por encontrar una solución política. El refuerzo a la eficacia extraterritorial del derecho fundamental a la protección de los datos personales de los ciudadanos europeos que se alcanzó con la sentencia Schrems no podía —ni debía—, sin embargo, dejar en situación de desamparo a las empresas europeas, que no gozaban de alternativas fáciles. Se hizo patente la necesidad urgente de un acuerdo político UE-EE.UU. que sustituyera al *Safe Harbor*. Y así ocurrió con la negociación y posterior aprobación por la Comisión Europea en julio de 2016 del acuerdo de adecuación para las transferencias de datos a EE.UU. denominado *Privacy Shield* (conocido en castellano como «Escudo de Privacidad»).

El acuerdo de *Privacy Shield* tenía como objetivo subsanar los principales defectos encontrados al acuerdo de *Safe Harbor* y que llevaron al Tribunal de Justicia de la Unión Europea a invalidar este sistema. Estos motivos, conforme se identifican y detallan en la sentencia del caso Schrems, eran fundamentalmente dos: la ausencia de un marco legislativo claro en EE.UU. para los casos en los que se restringen los derechos y libertades de los ciudadanos europeos en materia de protección de datos (p. ej., por motivos de seguridad nacional), así como la ausencia de mecanismos judiciales y de control efectivos que permitan a los ciudadanos europeos ejercitar sus derechos en ese país. El nuevo acuerdo UE-EE.UU. de escudo de privacidad (*Privacy Shield*) se articula, por tanto, alrededor de una serie de principios, todos ellos válidos, beneficiosos y acordes con la normativa europea de protección de datos, que buscan subsanar los defectos del sistema de *Safe Harbor*. Estos principios se pueden resumir en los siguientes:

— El derecho del ciudadano europeo a ser informado sobre los tratamientos de los datos.

— El establecimiento de limitaciones al uso de los datos con distintos fines de aquellos para los que se recogieron los datos legítimamente.

— El respeto al principio de minimización de los datos y la obligación de conservar los datos únicamente durante el tiempo necesario.

— La obligación de tratar los datos mediante sistemas seguros.

— La obligación de proteger los datos en el caso de que se transfieren a otra entidad.

— El reconocimiento y, sobre todo, la efectividad del derecho de los ciudadanos europeos a acceder a los datos y a su rectificación.

— El derecho a presentar una reclamación y a obtener reparación en caso de incumplimiento de estos principios.

Tras un complicado periodo —el que transcurrió entre la publicación de la sentencia del caso Schrems en octubre de 2015 y el mes de julio de 2016— sin un marco regulatorio básico para los flujos de datos transoceánicos, las empresas han visto cómo el acuerdo de *Privacy Shield* vino a resolver esta indefinición legal. Las transferencias de datos entre empresas y organizaciones de la Unión Europea y aquellas entidades estadounidenses adheridas al *Privacy Shield* se consideran realizadas a entidades que proporcionan un nivel de protección «adecuado» y, por tanto, son acordes al Derecho de la Unión Europea y sus Estados miembros. Sin embargo, el acuerdo de *Privacy Shield* ha estado acompañado, antes incluso de su aprobación, de polémica y de opiniones algo escépticas sobre su efectividad real en la protección de los derechos y libertades de los ciudadanos europeos. Actores esenciales en materia de protección de datos personales, como son el Parlamento Europeo, el Grupo

de Trabajo del Artículo 29 o el Supervisor Europeo de Protección de Datos, han emitido en diversas ocasiones opiniones e informes en los que han puesto de manifiesto algunas críticas respecto a la suficiencia del acuerdo alcanzado entre la UE-EE.UU.

Entre las opiniones más recientes encontramos la del Parlamento Europeo, que en enero de 2017 publicó un documento de análisis detallado[3] (*in-depth analysis*) de las ventajas —y algunas debilidades y retos— que, trascurridos unos meses desde su aprobación e implementación, surgen en su opinión del acuerdo de *Privacy Shield*. El informe del Parlamento Europeo destaca positivamente el que a pesar de que diversos principios del acuerdo de *Privacy Shield* parecen similares a los recogidos en el previo acuerdo de *Safe Harbor*, el nuevo marco regulador de los flujos transfronterizos incluye cambios significativos a las obligaciones que asumen aquellas entidades estadounidenses que deciden adherirse al escudo de privacidad. Estos cambios suponen un avance notable en la protección del derecho fundamental a la protección de datos personales. El Parlamento Europeo destaca, por ejemplo y entre otros muchos, cómo el acuerdo de *Privacy Shield* refuerza el derecho de los ciudadanos a decidir sobre determinados tratamientos, como puede ser el tratamiento para fines de *marketing* directo (*principle of choice*), reconociendo el derecho de los ciudadanos a decidir sobre si consienten el tratamiento de sus datos para finalidades significativamente distintas a aquellas para las que se recogieron sus datos, incluso si esas finalidades son compatibles con los originales. A estos reconocimientos el Parlamento Europeo le suma algunas objeciones, como, siguiendo con el ejemplo anterior, el hecho de que el acuerdo no establezca más claramente los plazos que deben otorgarse para que los ciudadanos puedan decidir sobre estos tratamientos —algo que, por otra parte, tampoco está resuelto en la normativa europea vigente de forma exhaustiva—. Sin embargo, los avances que supone el *Privacy Shield* frente al marco anterior no pueden ser, en conjunto, menospreciados.

El documento de análisis del Parlamento Europeo recoge también algunos de los retos a los que se enfrenta el acuerdo *Privacy Shield* en el futuro más próximo. Entre ellos, se destacan la necesidad de revisar de forma periódica la implementación real y la efectividad de los compromisos asumidos por los Gobiernos y las empresas al amparo del acuerdo —algo especialmente relevante tras el reciente cambio de Gobierno en EE. UU. y el anuncio de determinadas medidas—, la necesidad de analizar el acuerdo para garantizar su adecuación al Reglamento General de Protección de Datos (Reglamento UE 2016/679), la incertidumbre sobre el futuro de las negociaciones del Tratado Transatlántico de Comercio e Inversiones (TTIP) o los retos del *brexit*, entre otros. Por otra parte, el Parlamento Europeo se hace eco de cierta tibieza en la adopción, por parte de las entidades estadounidenses, de los principios del *Privacy Shield*. Tras varios meses desde su aprobación, el número de entidades estadounidenses adheridas al sistema sigue siendo significativamente inferior al número que se encontraba adherido al *Safe Habor*.

Con todo, la adopción del *Privacy Shield* ha supuesto un avance en la protección de los datos personales respecto del acuerdo de *Safe Harbor* y ha otorgado un marco jurídico concreto a las transferencias internacionales UE-EE.UU. Las distintas opiniones y las críticas vertidas sobre algunos de sus contenidos deben verse como una oportunidad para la mejora de su implementación y efectividad. Pero, por razones de seguridad jurídica y por la relevancia de los flujos de económicos y de datos entre ambos territorios, es crucial que exista un marco jurídico habilitador de flujos transoceánico de datos y que dicho marco goce de estabilidad. Para que los ciudadanos europeos se aseguren un nivel adecuado de protección y las empresas europeas y estadounidenses puedan desarrollar su actividad y relaciones en un marco jurídico seguro, es necesario dotar de seguridad y estabilidad a los acuerdos. Nadie duda de la existencia de retos para la supervivencia del acuerdo de *Privacy Shield*, pero es igualmente indudable que la inexistencia de un marco jurídico volvería a dejar en una situación de riesgo la protección de los derechos y libertades de los ciudadanos y empresas europeos. Por ello, el compromiso político y empresarial con la vigencia y efectividad de este y cualquier otro acuerdo que se alcance con impacto en los flujos de datos se hace esencial. Lo contrario supondría un precio alto a pagar por parte de los ciudadanos y las empresas.

3 http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf