ASUNTO C-311/18 "SCHREMS II": GUÍA SOBRE TRANSFERENCIAS INTERNACIONALES E INTERROGANTES ACTUALES EN RELACIÓN CON LAS TRANSFERENCIAS A TERCEROS PAÍSES

2 de octubre de 2020

El pasado 16 de julio de 2020, el Tribunal de Justicia de la UE ("*TJUE*") publicó su sentencia sobre el asunto C-311/18, en relación con la petición de decisión prejudicial planteada por el Tribunal Superior de la República de Irlanda. Las once cuestiones prejudiciales que fueron planteadas por el Tribunal Superior irlandés al TJUE giraban en torno a la compatibilidad del marco jurídico estadounidense con los derechos fundamentales recogidos en la Carta de los Derechos Fundamentales de la Unión Europea, así como instaban al TJUE a pronunciarse sobre la validez de las transferencias internacionales de datos personales a los Estados Unidos ("*EEUU*").

A través de dicha sentencia, y en respuesta a las cuestiones prejudiciales planteadas por el tribunal irlandés, el TJUE observó que existían diferencias sustanciales entre el marco de privacidad de la UE y el estadounidense, además de la existencia de normativa federal en EEUU en materia de seguridad nacional que no ofrecía garantías adecuadas para los ciudadanos europeos y procedió a anular la Decisión de la Comisión (UE) 2016/1250 de 12 de julio de 2016 por la que se aprobó el Escudo de Privacidad (o "*Privacy Shield*").

Asimismo, el TJUE, que mantuvo la validez de las Cláusulas Contractuales Tipo aprobadas por la Comisión Europea, recordó que las mismas únicamente tendrán validez si se adoptan "medidas adicionales" y suficientes a fin de garantizar la protección de los datos personales objeto de transferencia. En este sentido, el TJUE recordó que Responsables y Encargados del tratamiento, y en su defecto, las autoridades de control debían suspender o poner fin a aquellas transferencias que debido a su naturaleza, contexto y marco jurídico del país en el que se ubica la empresa receptora de datos personales, pudiese poner en entredicho las garantías anteriores.

La decisión del TJUE en el Asunto Schrems II, y la ausencia de un mecanismo actual que ofrezca garantías legítimas para transferir datos

personales a EEUU en sustitución del ya anulado Escudo de Privacidad ha propiciado que exista inseguridad jurídica en particular en aquellas empresas cuya actividad implica la subcontratación de servicios Cloud o hosting con empresas tecnológicas ubicadas en Estados Unidos.

En vista de lo anterior, el objeto de este análisis se centrará en definir el régimen legal por el que se regulan las transferencias internacionales de datos, describir los motivos por los que el TJUE anuló el Escudo de Privacidad, y posteriormente, analizar el impacto de la sentencia en el marco de las transferencias internacionales, analizar las principales alternativas vigentes para transferir datos a terceros países, e informar sobre las posturas que han adoptado las autoridades de control tras la publicación de la Sentencia.

1. ¿Qué es una transferencia internacional de datos personales?

El reglamento general de protección de datos ("RGPD"), entiende que existe una transferencia internacional de datos cuando los datos personales titularidad de un Responsable (la persona física o jurídica que determina los medios y finalidades del tratamiento) o Encargado (la persona física o jurídica que trata datos personales por cuenta de un Responsable) del tratamiento son remitidos a un tercero ubicado en un país fuera del Espacio Económico Europeo ("EEE") para que los pueda tratar en calidad de Responsable (mediante una cesión o comunicación de datos) o Encargado (mediante un acceso a datos personales en el marco de la prestación de un servicio concreto) del tratamiento.

En la actualidad, las transferencias internacionales de datos personales se han convertido en escenarios especialmente comunes, si bien en la mayoría de los casos tienen lugar de forma indirecta. A modo de ejemplo la irrupción de la tecnología Cloud (computación en la nube) de la que actualmente dependen un gran número de empresas debido a las ventajas en materia de almacenamiento y disponibilidad que ofrece esta tecnología, puede implicar el alojamiento de información en centros de datos concretos ubicados fuera del EEE. De esta manera, al producirse por tanto un acceso por parte de un tercero ubicado fuera del EEE a datos personales de un Responsable o Encargado del tratamiento en la Unión, existiría una transferencia internacional de datos personales sujeta al régimen que prevé la normativa de protección de datos.

2. ¿Cuál es el régimen normativo aplicable a las transferencias internacionales de datos?

De conformidad con el Reglamento General de Protección de Datos, solo se podrán realizar transferencias internacionales a entidades:

2.1 Ubicadas en un país reconocido como seguro mediante Decisión de adecuación de la Comisión Europea.

El RGPD autoriza de manera expresa las transferencias internacionales de datos a terceros ubicados en países reconocidos como seguros a través de una Decisión de adecuación de la Comisión Europea. Las decisiones europeas son normas jurídicas dirigidas a un destinatario concreto (en este caso, países concretos de fuera de la EEE), a quien a su vez, vinculan.

Las Decisiones de adecuación requieren de una evaluación previa por parte de la Comisión sobre el nivel de protección del tercer país al que van a vincular. En particular, las decisiones de adecuación deberán tener en cuenta el Estado de Derecho y el respeto a los derechos y libertades fundamentales, la legislación pertinente, el acceso de las autoridades públicas a los datos personales, la existencia de una o varias autoridades de control independientes, y el reconocimiento a los interesados cuyos datos personales son objeto de transferencia de derechos efectivos y exigibles así como de recursos administrativos y acciones judiciales que sean efectivas, entre otros criterios.

Por tanto, las empresas que necesiten llevar a cabo una transferencia internacional de datos, ya sea de forma directa o indirecta, deberán verificar que el país en el que se ubica el receptor de la información ha sido objeto de una Decisión por parte de la Comisión Europea. En caso de que el país en cuestión haya sido reconocido por la Comisión Europea como adecuado, se podrá llevar a cabo la transferencia internacional de datos sin necesidad de legitimar expresamente la

propia transferencia internacional. Cabe indicar que la decisión de adecuación únicamente autoriza o legitima la transferencia internacional *per se*, debiendo por tanto las empresas regular debidamente el acceso o comunicación de datos al tercero ubicado en un país fuera de la EEE conforme al resto de obligaciones que exige la normativa aplicable.

En fecha del presente Análisis, los países objeto de Decisión por parte de la Comisión en materia de adecuación son: a) Suiza; b) Canadá; c) Argentina; d) Guernesey; e) Isla de Man; f) Jersey; g) Islas Feroe; h) Andorra; i) Israel; j) Uruguay; k) Nueva Zelanda y l) Japón.

2.2 Que ofrezcan garantías adecuadas

A fin de legitimar las transferencias internacionales con terceros ubicados en países fuera de la EEE no reconocidos como adecuados por la Comisión Europea, el RGPD prevé mecanismos que ofrecen garantías adecuadas que incluyen pero no se limitan a que los interesados cuenten con derechos exigibles y con acciones legales efectivas, como forma de legitimar tales transferencias. En total, se prevén hasta cinco mecanismos de garantías adecuadas, siendo los más comunes:

(i) La suscripción de Cláusulas Contractuales Tipo adoptadas por la Comisión Europea entre la entidad emisora y la entidad receptora ubicada fuera de la EEE. Las Cláusulas Contractuales Tipo, aprobadas por la Comisión Europea mediante Decisión 2010/87 de 5 de febrero, son un documento cuyos términos y condiciones ofrecen, a ojos de la Comisión Europea, garantías adecuadas para tanto la protección de la privacidad como para los derechos fundamentales de los interesados cuyos datos personales son transferidos internacionalmente. De esta manera, la suscripción de dicho documento por ambas partes implicaría la legitimación de la transferencia internacional a través de la adquisición de las obligaciones contractuales que se detallan en dicho documento.

(ii) La adopción de Normas Corporativas Vinculantes sujetas a la aprobación por parte de la autoridad de control competente. Las Normas Corporativas Vinculantes implican la aceptación de las políticas, compromisos, y obligaciones en materia de protección de datos por parte de todas las entidades dentro de un mismo grupo empresarial o unión de empresas. El objetivo por tanto de las Normas Corporativas Vinculantes es garantizar un tratamiento adecuado de datos personales con independencia del país en el que se encuentre la entidad del grupo empresarial.

2.3 Mediante la aplicación de alguna de las excepciones para situaciones específicas previstas en el RGPD

En ausencia de tanto una decisión de adecuación por parte de la Comisión, como de la adopción de mecanismos que aportan garantías adecuadas para legitimar una transferencia internacional, el RGPD contempla una serie de excepciones tasadas bajo las cuales se podrá llevar a cabo dicha transferencia internacional:

(i) Si el interesado otorga su consentimiento explícito a la transferencia tras haber sido informado de los posibles riesgos de dichas transferencias;

(ii) La transferencia es necesaria para la ejecución de un contrato o para la ejecución de medidas precontractuales adoptada a solicitud del interesado;

(iii) La transferencia es necesaria para la ejecución de un contrato en interés del propio interesado;

(iv) La transferencia es necesaria por razones de interés público;

(v) La transferencia es necesaria para la formulación, ejercicio o la defensa de reclamaciones;

(vi) La transferencia es necesaria para proteger los intereses vitales del interesado o terceros cuando el interesado esté incapacitado para dar su consentimiento;

(vii) la transferencia se realice desde un registro público cuyo objeto sea facilitar información al público y esté abierto a la consulta del público en general o de cualquiera que acredite un interés legítimo.

Sin perjuicio de las anteriores excepciones, cabe recordar que el uso de la excepción relativa al interés público debe ser previamente reconocido por el derecho europeo o nacional. Asimismo, el uso de las excepciones relativas a la ejecución de un contrato, precontrato o reclamación, independientemente del procedimiento que fuere, únicamente podrán realizarse si la transferencia es ocasional y necesaria.

2.4 Si la transferencia no es repetitiva, afecta solo a un número limitado de interesados y es necesario para los intereses legítimos del Responsable o Encargado del tratamiento.

Por último, en caso de que no existiese decisión de adecuación, y en ausencia de garantías suficientes y excepciones aplicables, el RGPD contempla la posibilidad de legitimar una transferencia internacional en aquellos casos en los que la transferencia no es repetitiva, afecta a un número limitado de interesados y es necesario para los intereses legítimos que persigue el Responsable o Encargado del tratamiento.

En este sentido, es preciso indicar que la evaluación del interés legítimo requiere de la ponderación de los intereses de dicho Responsable o Encargado frente a los derechos y libertades del interesado, debiendo prevalecer los primeros. Asimismo, recurrir a este mecanismo implica a su vez la evaluación de todas las circunstancias concurrentes en la transferencia de datos, debiendo ofrecer garantías apropiadas basadas en dicha evaluación y debiendo, en cualquier caso, informar a la autoridad de control sobre la misma.

3. ¿Cómo se regulaban las transferencias internacionales a EEUU con anterioridad a la Sentencia del TJUE sobre el Asunto Schrems II?

Con anterioridad a la Sentencia del TJUE, las transferencias de datos personales a entidades de EEUU se consideraban adecuadas en aquellos casos en los que la entidad estadounidense receptora de los datos en cuestión estuviese adherida al Escudo de Privacidad. El Escudo de Privacidad fue adoptado a nivel Europeo a través de la Decisión 2016/1250 de la Comisión. Su objetivo era por un lado garantizar la seguridad de los datos de ciudadanos europeos que eran tratados en los EEUU y por otro, sustituir el antiguo acuerdo de Puerto Seguro que legitimaba las transferencias a EEUU y que fue también invalidado por el TJUE mediante Sentencia Asunto Schrems I, predecesora de la actual sentencia. Por tanto, y al contrario que el resto de Decisiones de adecuación suscritas en fecha de hoy, la Decisión 2016/1250 no reconocía al conjunto de EEUU como país seguro, sino a los términos y condiciones del Escudo de Privacidad, y por ende, a aquellas empresas que se adhiriesen a dichos términos y condiciones.

El Escudo de Privacidad disponía de medidas en materia de protección de datos (procedimientos de reclamación, derecho de información, o derecho a la supresión de datos, entre otros) que debían ser garantizadas por cualquier entidad que desease certificarse o adherirse a dicho mecanismo. La adhesión por parte de las empresas estadounidenses era voluntaria y estaba sujeta a una inspección posterior por parte de la autoridades estadounidenses. Tras validar el cumplimiento por parte de una empresa de las medidas requeridas por el Escudo de Privacidad, se procedía a incorporar a dicha empresa en una lista pública, a fin de certificar que la entidad garantizaba las medidas exigidas por tal mecanismo.

De esta manera, las empresas adheridas debidamente al Escudo de Privacidad disponían de legitimación suficiente para llevar a cabo transferencias internacionales, mientras que aquellas empresas estadounidenses no adheridas a dicho mecanismo debían recurrir a los mecanismos alternativos previstos por la normativa para llevar a cabo transferencias internacionales de datos.

4. ¿Por qué ha anulado el TJUE el Escudo de Privacidad de EEUU?

En su sentencia, el TJUE hace énfasis en las sustanciales diferencias entre las legislaciones estadounidense y europea en materia de privacidad y de derechos fundamentales como argumento principal por el que anula el Escudo de Privacidad. En particular, el TJUE observa que las entidades adheridas al Escudo de Privacidad no estarían exentas del cumplimiento con las obligaciones legales estadounidenses en materia de seguridad nacional (en particular, el cumplimiento de las secciones 702 de FISA y de

la EO 12333), que permiten el acceso de a datos personales por parte de las autoridades estadounidenses (en particular, de las autoridades encargadas de velar por la seguridad nacional de EEUU). Acceso que indica el TJUE se produciría sin respetar necesariamente el principio de proporcionalidad, en la medida en que las actuaciones de las autoridades con base a las anteriores normas federales no se limitan a lo estrictamente necesario.

De esta manera, entiende el TJUE que el acceso desproporcionado por parte de las autoridades estadounidenses a datos personales sin límite, unido a la ausencia de derechos, recursos y/o acciones judiciales exigibles por parte de los interesados europeos con respecto a tales autoridades provoca que el Escudo de Privacidad carezca de medidas suficientes que garanticen el cumplimiento de los derechos fundamentales de los interesados europeos.

Adicionalmente, el TJUE observó que el Defensor del Pueblo, figura creada para facilitar el proceso de respuesta a solicitudes de acceso de interesados europeos en materia de seguridad nacional en el ámbito del Escudo de Privacidad, no gozaba de independencia al depender del ejecutivo estadounidense. Además, el tribunal observó que no existían evidencias suficientes como para entender que el Defensor del Pueblo estuviese facultado para tomar decisiones vinculantes. Lo anterior llevó al TJUE a la conclusión de que el Defensor del Pueblo del Escudo de Privacidad realmente no proporcionaba ninguna vía de recurso ante un órgano que ofrezca a los interesados garantías sustancialmente equivalentes a las exigidas a través de la Carta de Derechos Fundamentales.

En vista de todo lo anterior, y al margen de que las empresas que se adhieren al Escudo de Privacidad aplican algunas medidas compatibles con la normativa europea, el TJUE, en vista de las injerencias sobre los derechos fundamentales que se seguían produciendo a raíz de la normativa estadounidense en materia de seguridad nacional estuviese la entidad dentro o fuera del Escudo de Privacidad, procedió a anular la Decisión 2016/1250 y con ello, el Escudo de Privacidad.

5. ¿Qué implicaciones tiene la Sentencia en lo que respecta a las transferencias internacionales de datos a países no reconocidos como adecuados por la Comisión?

5.1 Para EEUU

La sentencia del TJUE es particularmente negativa en lo que respecta a las futuras transferencias internacionales que realicen las empresas a entidades ubicadas en EEUU, al indicar el TJUE expresamente que el derecho estadounidense actual no garantiza un nivel de protección sustancialmente equivalente al europeo.

La anulación de la Decisión que creaba el Escudo de Privacidad, unido a las conclusiones específicas del TJUE sobre el derecho estadounidense conllevan asimismo un problema adicional a la hora de recurrir a garantías adecuadas como la suscripción de Cláusulas Contractuales Tipo y/o Normas Corporativas Vinculantes: la necesidad de llevar a cabo un análisis de equivalencia sobre un marco legislativo abiertamente reconocido por el TJUE como no seguro será difícilmente favorable.

En este sentido, y a fin de entender lo anterior, es preciso revelar que en la Sentencia Schrems II, el TJUE, además de anular el Escudo de Privacidad, siguió la opinión del Abogado General de diciembre de 2019, reconociendo que corresponde al Responsable o Encargado del tratamiento comprobar caso por caso (mediante un análisis de equivalencia) si el derecho del tercer país de destino es capaz de garantizar una protección adecuada de los datos personales transferidos. En este sentido, el TJUE recuerda que en ausencia de garantías por parte del tercer país de destino, el Responsable o Encargado deberá proporcionar medidas adicionales a las ofrecidas por las Cláusulas Contractuales Tipo o Normas Corporativas Vinculantes a fin de lograr la protección adecuada de los datos objeto de transferencia.

El TJUE a su vez, refrendando de nuevo la opinión del Abogado General, reconoció abiertamente que dicho Responsable o encargado del Tratamiento, y en su defecto, la autoridad de control competente, estarían obligados a suspender la transferencia al país tercero del que se trate cuando la misma no reuniese las

garantías adicionales que determinase dicho análisis.

Por tanto, y en vista de la obligación anterior aplicable para todo tipo de garantías adecuadas, incluidas las Normas Corporativas Vinculantes, la realización de un análisis de equivalencia favorable sobre el derecho estadounidense tras las conclusiones que hace el TJUE en Schrems II sobre el ordenamiento jurídico de dicho país parece en la actualidad, complejo.

5.2 Para el resto de los países fuera de la EEE que no han sido reconocidos como seguros por la Comisión Europea.

La norma de "equivalencia sustancial" descrita en el apartado anterior que señala la Sentencia deben tener las garantías adecuadas para legitimar las transferencias internacionales mediante este tipo de mecanismos obligará a Responsables, Encargados y autoridades de control competente a adoptar un papel proactivo en el estudio e identificación de cuáles son las medidas adicionales suficientes a adoptar para garantizar un adecuado nivel de protección de datos por parte de las entidades ubicadas fuera de la EEE que recibirán los datos personales.

Asimismo, la norma anterior obligará a Responsables y a Encargados a colaborar durante la realización del análisis de equivalencia, con el fin de identificar las obligaciones en el derecho del país receptor que pondrían en riesgo la transferencia internacional y subsiguientemente determinar las medidas alternativas para garantizar dicha equivalencia.

Sin perjuicio de lo anterior, y tras lo expuesto por el TJUE en el Asunto Schrems II sobre el derecho estadounidense, la elaboración de un análisis de equivalencia que arroje conclusiones positivas puede ser complejo en aquellos países que dispongan de una normativa en materia de seguridad nacional análoga a la de EEUU, como puede ser el caso de Reino Unido, cuyo '*Investigatory Powers Act 2016*' amenaza con complicar el régimen de transferencias internacionales con dicho país una vez finalice el periodo de transición previsto en su acuerdo de salida de la UE.

6. ¿Qué riesgos deben tener en cuenta las empresas que durante este periodo transicional decidan recurrir a las excepciones que prevé el RGPD?

Como se expuso anteriormente en el apartado 2.3 de este Análisis, en ausencia de una decisión de adecuación, y ante la imposibilidad de ofrecer garantías adecuadas con independencia si dicha imposibilidad tiene origen en la no superación del análisis de equivalencia o en la suspensión por parte de la autoridad de control de un mecanismo de garantías adecuadas, las entidades que transfieran datos personales a terceros países fuera de la EEE podrían recurrir en la aplicación de una de las excepciones que prevé la normativa.

Sin embargo, y como también se expuso anteriormente, las entidades que recurran a la aplicación de excepciones tales como la ejecución de un contrato o un precontrato deben tener en cuenta las interpretaciones que hace el Comité Europeo de Protección de Datos sobre los conceptos de "necesidad" y "transferencias ocasionales" con carácter previo a aplicar esta excepción. En este sentido, entiende el Comité que el criterio de "necesidad" exige de una relación estrecha y sustancial entre la transferencia de datos y el propio objeto del contrato. Asimismo, el elemento de "transferencia ocasional" ha de interpretarse en el sentido de que la transferencia pueda ocurrir más de una vez pero no de forma regular, en circunstancias aleatorias y a intervalos de tiempo arbitrarios.

La definición de los anteriores criterios resultará además de aplicación para las transferencias basadas en la formulación, ejercicio o defensa de reclamaciones, debiéndose sustituir el concepto de "necesidad" contractual anterior por la existencia de una relación estrecha y sustancial entre los datos en cuestión y el establecimiento, ejercicio o la defensa de la posición jurídica.

El consentimiento por su parte no requiere de los elementos anteriores, estando sujeto a la concurrencia de tres requisitos para que el mismo sea válido:

i. El consentimiento debe ser explícito;
ii. Ha de ser específico para la transferencia o serie de transferencias que vaya a tener

lugar con carácter previo al inicio de la transferencia

iii. El interesado ha de ser informado sobre los riesgos de la transferencia, inclusive del hecho de que la transferencia se realiza a un país que no ofrece un nivel adecuado de protección ni se prevén garantías adecuadas para la protección de sus datos.

Sin perjuicio de lo anterior, las directrices en materia de excepciones para la transferencia internacional de datos personales del Comité Europeo de Protección de Datos aclaran que el recurso de las excepciones no debe conducir a una situación en la que se puedan conculcar derechos fundamentales. A tal efecto, el uso de la excepción del consentimiento podría estar supeditada al riesgo de que la autoridad de control interprete dicho consentimiento como un mecanismo inválido en aquellos casos en los que existan sentencias que abiertamente reconozcan que concurre cierta injuria en los derechos fundamentales de la UE, como sería el caso de EEUU. Dicho riesgo podría incluso existir en los casos en los que el consentimiento se recogiese conforme a las propias directrices del Comité Europeo de Protección de Datos.

7. ¿Existen directrices o guías en la actualidad que definan las medidas complementarias que deben adoptarse en los mecanismos de garantías adecuadas?

En la actualidad, el Comité Europeo de Protección de Datos ha indicado que las medidas complementarias adicionales a incluir en los mecanismos de garantías adecuadas deben analizarse caso por caso, teniendo en cuenta las circunstancias concretas de la transferencia así como la legislación del país al que se pretenden transferir los datos personales.

El Comité Europeo de Protección de Datos a su vez ha anunciado que está estudiando los efectos e implicaciones de la sentencia con el fin de facilitar indicaciones adicionales sobre la naturaleza y forma que podrán adoptar las medidas adicionales.

En lo que respecta a las autoridades de control competentes, la autoridad alemana de la región de Baden-Württemberg ha publicado en septiembre directrices en las que indican como medidas complementarias a aplicar por las empresas sujetas a su jurisdicción el uso de medidas de encriptación y anonimización a fin de prevenir la identificación de los interesados por parte de las entidades estadounidenses y por tanto, la comunicación de datos personales como tal a las autoridades y órganos norteamericanos en virtud de la normativa federal anteriormente expuesta.

8. Ante la ausencia de directrices, ¿Pueden las entidades seguir transfiriendo datos a EEUU sin superar el análisis de equivalencia? ¿Qué requisitos y riesgos deben tenerse en cuenta?

El Comité Europeo de Protección de Datos y el propio TJUE han indicado que las entidades que deseen proseguir con la transferencia de datos personales incluso en aquellos casos en los que no se supere el análisis de equivalencia deberán notificarlo a la autoridad de control competente a fin de que puedan auditar al destinatario de la transferencia y comprobar si es preciso suspender o prohibir la transferencia en cuestión.

9. ¿Cómo han reaccionado las principales autoridades de control ante la sentencia Schrems II?

La recepción de la Sentencia Schrems II por parte de las autoridades de control ha sido inicialmente positiva, en tanto todas las autoridades han reconocido la sentencia y seguido las directrices que publicó el Comité Europeo de Protección de Datos a fin de mantener informadas a las empresas que tratan datos personales dentro de sus respectivas jurisdicciones.

Sin perjuicio de lo anterior, tras aproximadamente dos meses y medio desde la publicación de la sentencia del TJUE, son varias las autoridades de control que han adoptado diferentes posturas a la hora de aplicar las conclusiones de la Sentencia Schrems II en sus respectivos territorios.

En primer lugar, varias autoridades de control, entre las que cabe destacar la autoridad de control irlandesa, han adoptado una posición más agresiva en lo que respecta a la aplicación de la sentencia. Dichas autoridades de control han amenazado con aplicar la sentencia en su sentido

literal instando a ciertas entidades a cesar en la transferencia de los datos personales a servidores ubicados en Estados Unidos.

Por otra parte, la autoridad de control británica ("ICO") parece haber optado por adoptar una postura más pragmática con respecto a la aplicación de la sentencia. A tal efecto y aunque la ICO recuerda a las entidades afectadas que las implicaciones de esta siguen siendo aplicables para los Responsables y Encargados de Reino Unido, parece ser más consciente de las implicaciones que conlleva la anulación del Escudo de Privacidad. Por ello, la ICO insta a los afectados a analizar las transferencias internacionales que Responsables o Encargados llevan a cabo, dejando entrever que mientras analizan los impactos de la sentencia, aplicarán una postura basada más en el riesgo y en la proporcionalidad que en la aplicación literal y estricta de la sentencia.

Por último, existen autoridades de control que lejos de adoptar una postura más o menos agresiva, han optado por proporcionar directrices preliminares a las entidades ubicadas en su territorio de competencia, todo ello sin perjuicio de las futuras directrices que pudiese implementar el Comité Europeo de Protección de Datos en un futuro. De esta manera, autoridades de control tales como la ya mencionada autoridad regional alemana de Baden-Württemberg indican que para impedir el efectivo acceso por parte de las autoridades estadounidenses a los datos personales transferidos de la UE, las "medidas adicionales" a aplicar podrían incluir técnicas de encriptación y anonimización sobre los datos objeto de transferencia, como se indicó anteriormente. Todo ello con el fin de que los datos no puedan ser identificados en ningún momento por la entidad estadounidense y por tanto, por las autoridades encargadas de velar por la seguridad nacional.

No obstante, la autoridad de control regional también parece indicar que no valdría cualquier técnica de encriptación sino aquellas lo suficientemente fuertes como para impedir el acceso a los datos personales encriptados por parte de las autoridades estadounidenses, incrementando por tanto el nivel de complejidad de la operativa. Además, la clave de encriptación únicamente debería poseerla el exportador ubicado en la UE y por tanto fuera del ámbito de la normativa estadounidense.

10. ¿Qué efectos ha producido en la actualidad la Sentencia Schrems II desde su publicación?

Tras la publicación de la sentencia Schrems II, y durante el mes de agosto de 2020, Maximilian Schrems, el denunciante del asunto Schrems II, hizo público que ha interpuesto durante el pasado mes de agosto 101 denuncias ante las distintas autoridades de control de los Estados Miembros de la UE (cinco de ellas, tramitadas ante la Agencia Española de Protección de Datos) por el uso de servicios propios de las entidades Facebook y Google.

Posteriormente, a finales del mes agosto, la autoridad de control irlandesa envió un requerimiento a Facebook para que el gigante tecnológico cesase en el envío de datos personales a servidores ubicados en EEUU, fomentándose de esta manera la alarma en tanto las principales empresas tecnológicas americanas como en los millones de clientes que dependen de sus servicios a diario.

11. Conclusiones

La Sentencia Schrems II por la cual se anula el Escudo de Privacidad y se ponen de manifiesto las sustanciales diferencias entre el derecho de la Unión y el estadounidense, así como se hace hincapié en la necesidad de realizar análisis de equivalencia puede fomentar un gran nivel de inseguridad jurídica si el Comité Europeo de Protección de Datos y/o las autoridades de control no publican directrices sobre la forma en la que se podrán llevar a cabo las transferencias internacionales a corto plazo.

En la actualidad, y con base a lo que se expone en la sentencia, las entidades que realicen, directa o indirectamente transferencias internacionales a terceros ubicados en países no reconocidos como seguros por la Comisión Europea deberán analizar la naturaleza, contexto y finalidades por las que llevan a cabo dichas transferencias y determinar si:

i. Cesar de inmediato en el envío de datos personales a dichos terceros en tanto no existan directrices que definan lo que

entienden las autoridades de control conforman las "medidas adicionales" a las que se refiere el TJUE;

ii. Elaborar un análisis de equivalencia en colaboración con el tercero ubicado en el país receptor de la información con el fin de verificar si tanto el tercero como el ordenamiento jurídico del país en el que se ubica permiten el cumplimiento de los mecanismos de garantías adecuadas previstos en la normativa;
iii. Notificar a las autoridades de control la intención de continuar con las transferencias internacionales al margen de lo expuesto en la sentencia del TJUE, exponiéndose a posibles actuaciones por parte de la autoridad de control competente, que podrán variar desde la auditoría de la propia transferencia internacional, a la suspensión inmediata de la transferencia, e incluso, a la sanción por el incumplimiento de la obligación del Responsable y Encargado de suspender dicha transferencia internacional en los casos más graves; o

iv. Hacer uso de una de las excepciones contempladas en el RGPD, sin perjuicio de que más allá de cumplir con los requisitos concretos aplicables a cada excepción se esté actuando asumiendo el riesgo de interpretación que pueda realizar la autoridad de control competente de tanto la concurrencia de los requisitos en las excepciones que se quieren aplicar como en el uso de las mismas, en particular, en aquellas situaciones en las que la propia excepción pudiese conducir a una situación en la que se pudiesen conculcar derechos fundamentales, como puso de manifiesto el TJUE el pasado mes de julio en su Sentencia sobre el Asunto C-311/18.

ONTIER

Departamento: Digital Law
Contactos:
Joaquín Muñoz – jmunoz@ontier.net
Álvaro Vidal – avidal@ontier.net