Análisis · 18 de mayo de 2026

← Anterior·Siguiente →

Schrems II, cinco años después

La sentencia que cambió el derecho de las transferencias internacionales de datos personales. Cinco años después, una parte considerable del despacho cotidiano europeo sigue operando como si nada hubiera ocurrido.

Para entendernos: El 16 de julio de 2020, durante una mañana de jueves, un tribunal europeo declaró ilegal una parte enorme de cómo las empresas mandaban tus datos a Estados Unidos. Cinco años después, casi nadie ha cambiado nada. Tu información sigue volando exactamente igual que entonces.

La sentencia que tardó tres horas en cambiar las reglas

El 16 de julio de 2020, hacia las diez y cuarto de la mañana hora de Luxemburgo, el Tribunal de Justicia de la Unión Europea hizo pública la sentencia del asunto C-311/18. En las tres horas siguientes, el régimen jurídico que sostenía la transferencia diaria de datos personales de Europa a Estados Unidos —el llamado Escudo de Privacidad, Privacy Shield en su denominación oficial— dejó de existir. Cuando los responsables de protección de datos europeos terminaron de comer ese día, el marco bajo el que sus empresas y administraciones operaban no servía ya.

La sentencia se conoce hoy como Schrems II, por Maximilian Schrems, el activista austriaco cuya denuncia contra Facebook Ireland la disparó. La denuncia, en lo concreto, se ocupaba de las transferencias entre Facebook Irlanda y Facebook Estados Unidos. La sentencia, en lo general, va mucho más allá: dicta cómo y bajo qué condiciones puede pasar a Estados Unidos cualquier dato personal recogido en territorio europeo.

Casi seis años después, el marco de reemplazo existe —el EU-US Data Privacy Framework, adoptado en julio de 2023— y está, también, bajo presión jurídica. Una nueva ronda Schrems se prepara. Mientras tanto, la pequeña y mediana empresa europea sigue usando servicios cloud estadounidenses para tareas cotidianas, en su mayor parte sin saber que la cuestión jurídica sobre la que descansan esos servicios sigue abierta.

Qué decía exactamente Schrems II

La sentencia se sostiene sobre tres piezas. La primera es la Carta de los Derechos Fundamentales de la Unión Europea, en particular sus artículos 7 (vida privada y familiar), 8 (protección de datos personales) y 47 (tutela judicial efectiva). La segunda es el Reglamento General de Protección de Datos —el RGPD que muchos europeos solo recuerdan por los avisos de cookies—, específicamente su capítulo V, artículos 44 a 50, sobre transferencias internacionales. La tercera es la legislación estadounidense de inteligencia: la sección 702 de la Foreign Intelligence Surveillance Act, FISA 702 en jerga jurídica, y la Orden Ejecutiva presidencial 12333.

El tribunal procedió por contraste. La Carta de Derechos Fundamentales exige que los datos personales de los ciudadanos europeos disfruten, cuando salen de la Unión, de un nivel de protección esencialmente equivalente al garantizado por el RGPD. La pregunta era, en consecuencia, si Estados Unidos ofrece ese nivel esencialmente equivalente.

La respuesta fue negativa, y no por matices. FISA 702 permite al gobierno estadounidense recabar comunicaciones de no estadounidenses ubicados fuera del territorio nacional sin autorización judicial individual

previa, sin notificación al afectado, y sin un recurso efectivo comparable al europeo. La Orden Ejecutiva 12333 amplía esa capacidad de manera análoga fuera del territorio nacional. El tribunal concluyó que el ciudadano europeo, ante el sistema jurídico estadounidense, no dispone de la protección esencialmente equivalente que la Carta exige. La equivalencia, por tanto, no existe.

De ahí la consecuencia directa: la Decisión 2016/1250 de la Comisión Europea, que había validado el Privacy Shield como marco adecuado para las transferencias, fue declarada inválida. Toda transferencia amparada únicamente en ese marco quedó sin base jurídica desde ese mismo instante.

Lo que sí sobrevivió (y bajo qué condiciones)

Schrems II no eliminó todos los instrumentos. Las Cláusulas Contractuales Tipo —los SCC en jerga internacional, por sus siglas inglesas Standard Contractual Clauses— sobrevivieron. Son contratos modelo aprobados por la Comisión Europea: un exportador europeo y un importador del país de destino los firman comprometiéndose a tratar los datos según el estándar europeo. La empresa que pensó haber resuelto el problema el día 17 de julio de 2020 firmó SCC con su proveedor y se dio por contenta.

La incomodidad llegó al leer la sentencia despacio. El tribunal dejó claro que las SCC siguen siendo válidas, pero su validez depende de una condición que conviene subrayar: que el importador del dato pueda cumplirlas en la práctica. Si la legislación nacional del país de destino le impide cumplir las cláusulas —porque, por ejemplo, una orden bajo FISA 702 le obliga a entregar los datos sin notificarlo a su contraparte europea—, las cláusulas no protegen en realidad. Y entonces, dice el tribunal, el exportador europeo debe suspender la transferencia.

Esto introdujo un nuevo objeto en la práctica europea de protección de datos: la Transfer Impact Assessment, o análisis de impacto de la transferencia, conocida por sus siglas inglesas TIA. Cada vez que una empresa europea quiere trasladar datos a Estados Unidos al amparo de SCC, debe evaluar formalmente si el destinatario puede cumplir las cláusulas dada la legislación que se le aplica. El Comité Europeo de Protección de Datos publicó orientaciones detalladas sobre cómo conducir la TIA. La práctica honesta suele dar el mismo resultado: si el importador es una filial estadounidense de un grande del cloud, la respuesta sincera a la TIA es que las cláusulas no se pueden cumplir como están escritas.

El Privacy Framework y el Schrems III pendiente

El 10 de julio de 2023, la Comisión Europea adoptó una nueva Decisión de Adecuación: la 2023/1795. Sustituye al difunto Privacy Shield y opera bajo el nombre EU-US Data Privacy Framework. Estados Unidos modificó previamente su régimen interno mediante la Orden Ejecutiva 14086, que limita el alcance de la inteligencia de señales al «necesario y proporcionado» —terminología familiar para el lector europeo, no tanto para la práctica administrativa estadounidense— y crea un órgano de revisión llamado Data Protection Review Court (DPRC). La Comisión consideró que estas modificaciones bastaban para restablecer el nivel esencialmente equivalente.

La organización noyb, fundada por Schrems, interpuso una denuncia el 7 de septiembre de 2023 contra la nueva Decisión. Los argumentos son los esperables: el DPRC no es un tribunal independiente en el sentido del artículo 47 de la Carta; los conceptos «necesario y proporcionado» no traducen mecánicamente los estándares europeos; y, finalmente, una protección que descansa sobre una Orden Ejecutiva puede ser revocada por la Orden Ejecutiva siguiente. Una sentencia del TJUE sobre la nueva Decisión —la que muchos llaman ya, con cierta resignación, Schrems III— se espera para los próximos años. El resultado no se puede anticipar. La estructura del argumento, en cualquier caso, recuerda mucho a la de 2020.

Lo que la PYME europea no oye

Mientras la gran sala del TJUE delibera, el despacho de abogados de tamaño mediano sigue intercambiando correspondencia con sus clientes a través de Microsoft 365 alojado en regiones europeas pero propiedad de una

empresa estadounidense sujeta a FISA 702. La consulta médica privada sincroniza agendas a través de Google Workspace. El asesor fiscal envía declaraciones firmadas mediante DocuSign. El psicólogo factura desde una hoja de cálculo en Notion. El bufete laboralista archiva expedientes en Dropbox. Y prácticamente todos ellos, además, atienden a sus clientes por WhatsApp. Todo esto puede operar amparado, según los proveedores, en la Decisión de Adecuación 2023/1795. El día en que esa Decisión caiga en Schrems III, todas esas relaciones quedan a la intemperie en el mismo segundo.

La cuestión no es retórica. Entre 2022 y 2024, varias autoridades europeas resolvieron expedientes contra responsables del tratamiento por usar Google Analytics sin instrumento adecuado de transferencia, en aplicación literal del razonamiento del TJUE incluso antes de que el Privacy Framework entrara en vigor. La autoridad francesa, la CNIL, fue la primera en formalizar el criterio en 2022; las autoridades austriaca, italiana y otras siguieron poco después. El incumplimiento, bajo el actual diseño operativo de la PYME europea, se documenta en tiempo real ante quien sepa mirar.

La TIA como instrumento, no como ritual

Una parte considerable de las TIA que circulan por despachos europeos son, leídas con atención, ejercicios formales. Listan los instrumentos contractuales, enumeran las certificaciones del proveedor, citan las garantías técnicas, marcan la casilla. Pocas se preguntan en serio si una orden FISA 702 obligaría al proveedor a entregar los datos. Aún menos se preguntan qué pasaría con esa transferencia bajo una hipotética revisión del Privacy Framework. El artículo 5 del RGPD exige al responsable del tratamiento ser capaz de demostrar el cumplimiento. Una TIA que no se hace en serio no demuestra nada; lo que demuestra es la voluntad de cumplir sobre el papel mientras se hace lo contrario en la práctica.

La versión sincera de la TIA arranca con una pregunta sencilla: ¿qué ocurriría si mañana le llegara a este proveedor una orden FISA 702 sobre estos datos concretos? Si la respuesta honesta es «tendría que entregarlos sin avisarnos», las cláusulas contractuales no resuelven el problema. Lo que sí lo resuelve, en los casos en los que la pregunta importa de verdad, es no haber puesto el dato en manos de ese proveedor.

El cambio político como riesgo estructural

Hay una capa adicional, política, que conviene nombrar sin dramatismo. La Decisión de Adecuación 2023/1795 descansa, en último término, sobre la Orden Ejecutiva 14086, firmada por el presidente Biden en octubre de 2022. Una Orden Ejecutiva la firma un presidente y la puede revocar, modificar o vaciar de contenido el siguiente. La protección de los datos europeos en Estados Unidos depende, así, de una decisión administrativa que ni el Congreso americano garantiza ni el sistema jurídico americano protege con la solidez con que protege otras materias internas. Desde enero de 2025 una nueva administración rige Estados Unidos, y la pregunta sobre la continuidad práctica de la EO 14086 ha dejado de ser una hipótesis para volverse contemporánea. Cualquier escenario en el que la administración decida retirar o atenuar la Orden dejaría a la Decisión Europea sin la pieza sobre la que se construyó.

No es un argumento conspirativo. Es la lectura sobria del diseño jurídico. Los marcos de protección de datos transatlánticos se han caído ya dos veces: el Safe Harbor en 2015 (sentencia Schrems I), el Privacy Shield en 2020 (Schrems II). El tercero descansa sobre una pieza más frágil que sus dos predecesores. Una empresa europea que apuesta hoy su tratamiento de datos a esa pieza está tomando una decisión de gestión del riesgo, no de mero cumplimiento normativo.

Para el lector profesional

Las preguntas operativas que conviene formularse antes de elegir un servicio cloud para datos profesionales —con el rigor con el que un inspector de protección de datos las plantearía— son las siguientes:

1. ¿Dónde se almacenan físicamente los datos? Una región europea no es respuesta suficiente si el operador es estadounidense.
2. ¿Quién opera el servicio, en qué jurisdicción está incorporado, y a qué órdenes legales puede ser sometido?
3. ¿Qué instrumento de transferencia se invoca: Decisión de Adecuación 2023/1795, SCC con TIA, derogación del artículo 49 del RGPD? ¿Es defendible esa elección ante una inspección?
4. Si la Decisión de Adecuación cayera mañana, ¿qué plan operativo existe para mantener la actividad?
5. ¿Existe una alternativa europea o autohospedada para esa función, y qué coste real tendría migrar?

No todas las funciones del despacho cotidiano requieren la misma respuesta. Una hoja de cálculo para contabilidad interna probablemente no eleva la pregunta a este nivel. El expediente penal de un cliente, el historial clínico, la nómina de los empleados, sí. La proporcionalidad es legítima; la inercia colectiva con la que la PYME europea ha permanecido en proveedores estadounidenses para todo —incluso para lo más sensible— no lo es.

Schrems II cumple seis años este julio. La sentencia no ha cambiado los hábitos cotidianos de la mayoría de empresas europeas. Ha cambiado, eso sí, el mapa de riesgos a los que esas empresas están expuestas. Cuando una decisión administrativa estadounidense se interpone entre el reglamento europeo y la operativa real de una PYME, conviene al menos saber que la decisión está ahí, y que es frágil. Quienes hayamos elegido una arquitectura sin operador en medio —el hilo que recorre Cuadernos Lacre— preferiríamos no tener que escribir esta clase de análisis cada vez que un Schrems se sienta a presentar un recurso. Pero seguiremos haciéndolos.

Nota editorial: cuando este Cuaderno nombra empresas o productos, no es para acusar. Quienes los construyen hacen trabajos que millones de personas usan y aprecian. Lo que señalamos es estructural — el modelo, no la marca. Las marcas aparecen como ejemplo porque son las que el lector reconoce.

Fuentes y lectura adicional

- Tribunal de Justicia de la Unión Europea — sentencia de 16 de julio de 2020, asunto C-311/18, *Data Protection Commissioner contra Facebook Ireland Ltd. y Maximillian Schrems*.
- Reglamento (UE) 2016/679, capítulo V, artículos 44 a 50 — transferencias internacionales de datos personales.
- Decisión de Ejecución (UE) 2023/1795 de la Comisión, de 10 de julio de 2023, sobre el nivel adecuado de protección de los datos personales en el marco del EU-US Data Privacy Framework.
- Comité Europeo de Protección de Datos — *Recomendaciones 01/2020 sobre las medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de datos personales de la UE*, adoptadas el 18 de junio de 2021.
- noyb.eu — denuncia interpuesta el 7 de septiembre de 2023 contra la Decisión (UE) 2023/1795 ante las autoridades europeas de protección de datos.
- *Foreign Intelligence Surveillance Act*, sección 702 (codificada en 50 U.S.C. § 1881a), y Orden Ejecutiva 12333 sobre actividades de inteligencia estadounidense fuera del territorio nacional.

← AnteriorCuando no hay nadie en medioSiguiente →Qué es realmente SHA-256

Lecturas recientes

- Análisis · 18 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse
- Análisis · 18 de mayo de 2026 Self-hosting como práctica profesional
- Concepto · 18 de mayo de 2026 Las 24 palabras: qué es una identidad criptográfica

Llévate este artículo donde lo necesites.

↓ Markdown ↓ Texto plano ↓ PDF

El archivo se descarga a tu dispositivo. Desde ahí puedes guardarlo, importarlo a Solo2, o compartirlo donde quieras. Cuadernos no decide el destino por ti.

Sello de lacre · SHA-256 a1cc46cbc6e57be29c414689c651002f98e04710b62ef3ef3572d4de640c65bb

Cuadernos Lacre · Una publicación de Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada por el equipo de Solo2.