Análise · 18 de maio de 2026

← Anterior·Seguinte →

Schrems II, cinco anos despois

A sentenza que mudou o dereito das transferencias internacionais de datos persoais. Cinco anos despois, unha parte considerable do despacho cotián europeo segue operando coma se nada houbese ocorrido.

Para entendernos: O 16 de xullo de 2020, durante unha mañá de xoves, un tribunal europeo declarou ilegal unha parte enorme de como as empresas mandaban os teus datos aos Estados Unidos. Cinco anos despois, case ninguén cambiou nada. A túa información segue voando exactamente igual que entón.

A sentenza que tardou tres horas en cambiar as regras

O 16 de xullo de 2020, cara ás dez e cuarto da mañá hora de Luxemburgo, o Tribunal de Xustiza da Unión Europea fixo pública a sentenza do asunto C-311/18. Nas tres horas seguintes, o réxime xurídico que sostiña a transferencia diaria de datos persoais de Europa a Estados Unidos —o chamado Privacy Shield (Escudo de Privacidade)— deixou de existir. Cando os responsables de protección de datos europeos terminaron de comer ese día, o marco baixo o que as súas empresas e administracións operaban xa non servía.

A sentenza coñécese hoxe como Schrems II, por Maximilian Schrems, o activista austríaco cuxa denuncia contra Facebook Ireland a disparou. A denuncia, no concreto, ocupábase das transferencias entre Facebook Irlanda e Facebook Estados Unidos. A sentenza, no xeral, vai moito máis alá: dita como e baixo que condicións pode pasar a Estados Unidos calquera dato persoal recollido en territorio europeo.

Case seis anos despois, o marco de substitución existe —o EU-US Data Privacy Framework, adoptado en xullo de 2023— e está, tamén, baixo presión xurídica. Unha nova rolda Schrems prepárase. Mentres tanto, a pequena e mediana empresa europea segue usando servizos cloud estadounidenses para tarefas cotiás, na súa maior parte sen saber que a cuestión xurídica sobre a que descansan eses servizos segue aberta.

Que dicía exactamente Schrems II

A sentenza sostense sobre tres pezas. A primeira é a Carta dos Dereitos Fundamentais da Unión Europea, en particular os seus artigos 7 (vida privada e familiar), 8 (protección de datos persoais) e 47 (tutela xudicial efectiva). A segunda é o Regulamento Xeral de Protección de Datos —o RGPD que moitos europeos só lembran polos avisos de cookies—, especificamente o seu capítulo V, artigos 44 a 50, sobre transferencias internacionais. A terceira é a lexislación estadounidense de intelixencia: a sección 702 da Foreign Intelligence Surveillance Act, FISA 702 en xerga xurídica, e a Orde Executiva presidencial 12333.

O tribunal procedeu por contraste. A Carta de Dereitos Fundamentais esixe que os datos persoais dos cidadáns europeos gocen, cando saen da Unión, dun nivel de protección esencialmente equivalente ao garantido polo RGPD. A pregunta era, en consecuencia, se Estados Unidos ofrece ese nivel esencialmente equivalente.

A resposta foi negativa, e non por matices. FISA 702 permite ao goberno estadounidense recadar comunicacións de non estadounidenses situados fóra do territorio nacional sen autorización xudicial individual previa, sen notificación ao afectado, e sen un recurso efectivo comparable ao europeo. A Orde Executiva 12333 amplía esa capacidade de xeito análogo fóra do territorio nacional. O tribunal concluíu que o cidadán europeo, ante o

sistema xurídico estadounidense, non dispón da protección esencialmente equivalente que a Carta esixe. A equivalencia, xa que logo, non existe.

De aí a consecuencia directa: a Decisión 2016/1250 da Comisión Europea, que validara o Privacy Shield como marco adecuado para as transferencias, foi declarada inválida. Toda transferencia amparada unicamente nese marco quedou sen base xurídica desde ese mesmo instante.

O que si sobreviviu (e baixo que condicións)

Schrems II non eliminou todos os instrumentos. As Cláusulas Contractuais Tipo —os SCC en xerga internacional — sobreviviron. Son contratos modelo aprobados pola Comisión Europea: un exportador europeo e un importador do país de destino asínanos comprometéndose a tratar os datos segundo o estándar europeo. A empresa que pensou resolver o problema o día 17 de xullo de 2020 asinou SCC co seu provedor e deuse por contenta.

A incomodidade chegou ao ler a sentenza amodo. O tribunal deixou claro que as SCC seguen sendo válidas, pero a súa validez depende dunha condición que convén subliñar: que o importador do dato poida cumprilas na práctica. Se a lexislación nacional do país de destino lle impide cumprir as cláusulas —porque, por exemplo, unha orde baixo FISA 702 o obriga a entregar os datos sen notificalo á súa contraparte europea—, as cláusulas non protexen na realidade. E entón, di o tribunal, o exportador europeo debe suspender a transferencia.

Isto introduciu un novo obxecto na práctica europea de protección de datos: a Transfer Impact Assessment, ou análise de impacto da transferencia, coñecida polas súas siglas inglesas TIA. Cada vez que unha empresa europea quere trasladar datos a Estados Unidos ao abeiro de SCC, debe avaliar formalmente se o destinatario pode cumprir as cláusulas dada a lexislación que se lle aplica. O Comité Europeo de Protección de Datos publicou orientacións detalladas sobre como conducir a TIA. A práctica honesta adoita dar o mesmo resultado: se o importador é unha filial estadounidense dun grande do cloud, a resposta sincera á TIA é que as cláusulas non se poden cumprir como están escritas.

O Privacy Framework e o Schrems III pendente

O 10 de xullo de 2023, a Comisión Europea adoptou unha nova Decisión de Adecuación: a 2023/1795. Substitúe ao difunto Privacy Shield e opera baixo o nome EU-US Data Privacy Framework. Estados Unidos modificou previamente o seu réxime interno mediante a Orde Executiva 14086, que limita o alcance da intelixencia de sinais ao «necesario e proporcionado» —terminoloxía familiar para o lector europeo, non tanto para a práctica administrativa estadounidense— e crea un órgano de revisión chamado Data Protection Review Court (DPRC). A Comisión considerou que estas modificacións bastaban para restablecer o nivel esencialmente equivalente.

A organización noyb, fundada por Schrems, interpuxo unha denuncia o 7 de setembro de 2023 contra a nova Decisión. Os argumentos son os esperables: o DPRC non é un tribunal independente no sentido do artigo 47 da Carta; os conceptos «necesario e proporcionado» non traducen mecanicamente os estándares europeos; e, finalmente, unha protección que descansa sobre unha Orde Executiva pode ser revogada pola Orde Executiva seguinte. Unha sentenza do TJUE sobre a nova Decisión —a que moitos chaman xa, con certa resignación, Schrems III— espérase para os vindeiros anos. O resultado non se pode anticipar. A estrutura do argumento, en calquera caso, lembra moito á de 2020.

O que a PEME europea non oe

Mentres a gran sala do TJUE delibera, o despacho de avogados de tamaño medio segue intercambiando correspondencia cos seus clientes a través de Microsoft 365 aloxado en rexións europeas pero propiedade dunha empresa estadounidense suxeita a FISA 702. A consulta médica privada sincroniza axendas a través de Google Workspace. O asesor fiscal envía declaracións asinadas mediante DocuSign. O psicólogo factura desde unha

folla de cálculo en Notion. O bufete laboralista arquiva expedientes en Dropbox. E practicamente todos eles, ademais, atenden aos seus clientes por WhatsApp. Todo isto pode operar amparado, segundo os provedores, na Decisión de Adecuación 2023/1795. O día en que esa Decisión caia en Schrems III, todas esas relacións quedan á intemperie no mesmo segundo.

A cuestión non é retórica. Entre 2022 e 2024, varias autoridades europeas resolveron expedientes contra responsables do tratamento por usar Google Analytics sen instrumento adecuado de transferencia, en aplicación literal do razoamento do TJUE incluso antes de que o Privacy Framework entrase en vigor. A autoridade francesa, a CNIL, foi a primeira en formalizar o criterio en 2022; as autoridades austríaca, italiana e outras seguiron pouco despois. O incumprimento, baixo o actual deseño operativo da PEME europea, documéntase en tempo real ante quen saiba mirar.

A TIA como instrumento, non como ritual

Unha parte considerable das TIA que circulan por despachos europeos son, lidas con atención, exercicios formais. Listan os instrumentos contractuais, enumeran as certificacións do provedor, citan as garantías técnicas, marcan a casa. Poucas se preguntan en serio se unha orde FISA 702 obrigaría ao provedor a entregar os datos. Aínda menos se preguntan que pasaría con esa transferencia baixo unha hipotética revisión do Privacy Framework. O artigo 5 do RGPD esixe ao responsable do tratamento ser capaz de demostrar o cumprimento. Unha TIA que non se fai en serio non demostra nada; o que demostra é a vontade de cumprir sobre o papel mentres se fai o contrario na práctica.

A versión sincera da TIA arranca cunha pregunta sinxela: que ocorrería se mañá lle chegase a este provedor unha orde FISA 702 sobre estes datos concretos? Se a resposta honesta é «tería que entregalos sen avisarnos», as cláusulas contractuais non resolven o problema. O que si o resolve, nos casos nos que a pregunta importa de verdade, é non ter posto o dato en mans dese provedor.

O cambio político como risco estrutural

Hai unha capa adicional, política, que convén nomear sen dramatismo. A Decisión de Adecuación 2023/1795 descansa, en último termo, sobre a Orde Executiva 14086, asinada polo presidente Biden en outubro de 2022. Unha Orde Executiva asínaa un presidente e pódea revogar, modificar o baleirar de contido o seguinte. A protección dos datos europeos en Estados Unidos depende, así, dunha decisión administrativa que nin o Congreso americano garante nin o sistema xurídico americano protexe coa solidez con que protexe outras materias internas. Desde xaneiro de 2025 unha nova administración rexe Estados Unidos, e a pregunta sobre a continuidade práctica da EO 14086 deixou de ser unha hipótese para volverse contemporánea. Calquera escenario no que a administración decida retirar ou atenuar a Orde deixaría á Decisión Europea sen a peza sobre a que se construíu.

Non é un argumento conspirativo. É a lectura sobria do deseño xurídico. Os marcos de protección de datos transatlánticos caeron xa dúas veces: o Safe Harbor en 2015 (sentenza Schrems I), o Privacy Shield en 2020 (Schrems II). O terceiro descansa sobre unha peza máis fráxil que os seus dous predecesores. Unha empresa europea que aposta hoxe o seu tratamento de datos a esa peza está tomando unha decisión de xestión do risco, non de mero cumprimento normativo.

Para o lector profesional

As preguntas operativas que convén formularse antes de elixir un servizo cloud para datos profesionais —co rigor co que un inspector de protección de datos as plantexaría— son as seguintes:

1. Onde se almacenan fisicamente os datos? Unha rexión europea non é resposta abondo se o operador é estadounidense.

2. Quen opera o servizo, en que xurisdición está incorporado, e a que ordes legais pode ser sometido?
3. Que instrumento de transferencia se invoca: Decisión de Adecuación 2023/1795, SCC con TIA, derrogación do artigo 49 do RGPD? É defendible esa elección ante unha inspección?
4. Se a Decisión de Adecuación caese mañá, que plan operativo existe para manter a actividade?
5. Existe unha alternativa europea ou autohospedada para esa función, e que custo real tería migrar?

Non todas as funcións do despacho cotián requiren a mesma resposta. Unha folla de cálculo para contabilidade interna probablemente non eleva a pregunta a este nivel. O expediente penal dun cliente, o historial clínico, a nómina dos empregados, si. A proporcionalidade é lexítima; a inercia colectiva coa que a PEME europea permaneceu en provedores estadounidenses para todo —incluso para o máis sensible— non o é.

Schrems II cumpre seis anos este xullo. A sentenza non mudou os hábitos cotiáns da maioría das empresas europeas. Mudou, iso si, o mapa de riscos aos que esas empresas están expostas. Cando unha decisión administrativa estadounidense se interpón entre o regulamento europeo e a operativa real dunha PEME, convén polo menos saber que a decisión está aí, e que é fráxil. Quen eliximos unha arquitectura sen operador polo medio —o fío que percorre Cuadernos Lacre— prefeririamos non ter que escribir esta clase de análise cada vez que un Schrems se senta a presentar un recurso. Pero seguiremos facéndoos.

Nota editorial: cando estes Cuadernos nomean empresas ou produtos, non é para acusar. Quenes os constrúen fan traballos que millóns de persoas usan e aprecian. O que sinalamos é estrutural — o modelo, non a marca. As marcas aparecen como exemplo porque son as que o lector recoñece.

Fontes e lectura adicional

- Tribunal de Xustiza da Unión Europea — sentenza de 16 de xullo de 2020, asunto C-311/18, *Data Protection Commissioner contra Facebook Ireland Ltd. e Maximillian Schrems*.
- Regulamento (UE) 2016/679, capítulo V, artigos 44 a 50 — transferencias internacionais de datos persoais.
- Decisión de Execución (UE) 2023/1795 da Comisión, de 10 de xullo de 2023, sobre o nivel adecuado de protección dos datos persoais no marco do EU-US Data Privacy Framework.
- Comité Europeo de Protección de Datos — *Recomendacións 01/2020 sobre as medidas que complementan os instrumentos de transferencia para garantir o cumprimento do nivel de protección de datos persoais da UE*, adoptadas o 18 de xuño de 2021.
- noyb.eu — denuncia interposta o 7 de setembro de 2023 contra a Decisión (UE) 2023/1795 ante as autoridades europeas de protección de datos.
- *Foreign Intelligence Surveillance Act*, sección 702 (codificada en 50 U.S.C. § 1881a), e Orde Executiva 12333 sobre actividades de intelixencia estadounidense fóra do territorio nacional.

← AnteriorCando non hai ninguén no medioSeguinte →Que é realmente SHA-256

Lecturas recentes

- Análise · 18 de maio de 2026 Privacidade real vs aparente: as preguntas que convén facerse
- Análise · 18 de maio de 2026 Self-hosting como práctica profesional
- Concepto · 18 de maio de 2026 As 24 palabras: que é unha identidade criptográfica

Leva este artigo onde o necesites.

↓ Markdown ↓ Texto plano ↓ PDF

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 36558f31298741abf32bd83aef3b04f959be6391dcf15d130743cac5bd51835d

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

Esta web no usa cookies e non carga recursos de terceiros. Usa un contador anónimo de visitas autohospedado (Umami, no noso servidor europeo) e o mínimo JavaScript necesario para os dous controis do cabezal: tema claro ou escuro, e selector de idioma. Sen trackers, sen perfilado, sen compartir datos. Se queres seguirnos: RSS.