Análise · 18 de maio de 2026

← Anterior·Seguinte →

Schrems II, cinco anos depois

A sentença que mudou o direito das transferências internacionais de dados pessoais. Cinco anos depois, uma parte considerável do quotidiano europeu continua a operar como se nada tivesse acontecido.

A sentença que demorou três horas a mudar as regras

Em 16 de julho de 2020, por volta das dez e um quarto da manhã, hora de Luxemburgo, o Tribunal de Justiça da União Europeia tornou pública a sentença do processo C-311/18. Nas três horas seguintes, o regime jurídico que sustentava a transferência diária de dados pessoais da Europa para os Estados Unidos — o chamado Escudo de Privacidade, Privacy Shield na sua denominação oficial — deixou de existir. Quando os responsáveis pela proteção de dados europeus terminaram de almoçar nesse dia, o quadro sob o qual as suas empresas e administrações operavam já não servia.

A sentença é hoje conhecida como Schrems II, em homenagem a Maximilian Schrems, o ativista austríaco cuja denúncia contra o Facebook Ireland a desencadeou. A denúncia, em concreto, tratava das transferências entre o Facebook Irlanda e o Facebook Estados Unidos. A sentença, em geral, vai muito mais além: dita como e sob que condições qualquer dado pessoal recolhido em território europeu pode passar para os Estados Unidos.

Quase seis anos depois, o quadro de substituição existe — o EU-US Data Privacy Framework, adotado em julho de 2023 — e está, também, sob pressão jurídica. Uma nova ronda Schrems prepara-se. Entretanto, a pequena e média empresa europeia continua a usar serviços cloud norte-americanos para tarefas quotidianas, na sua maioria sem saber que a questão jurídica sobre a qual assentam esses serviços continua aberta.

O que dizia exatamente o Schrems II

A sentença baseia-se em três peças. A primeira é a Carta dos Direitos Fundamentais da União Europeia, em particular os seus artigos 7 (vida privada e familiar), 8 (proteção de dados pessoais) e 47 (tutela jurisdicional efetiva). A segunda é o Regulamento Geral sobre a Proteção de Dados — o RGPD que muitos europeus apenas recordam pelos avisos de cookies —, especificamente o seu capítulo V, artigos 44 a 50, sobre transferências internacionais. A terceira é a legislação norte-americana de inteligência: a secção 702 da Foreign Intelligence Surveillance Act, FISA 702 no jargão jurídico, e a Ordem Executiva presidencial 12333.

O tribunal procedeu por contraste. A Carta dos Direitos Fundamentais exige que os dados pessoais dos cidadãos europeus gozem, quando saem da União, de um nível de proteção essencialmente equivalente ao garantido pelo RGPD. A questão era, consequentemente, se os Estados Unidos oferecem esse nível essencialmente equivalente.

A resposta foi negativa, e não por detalhes. A FISA 702 permite ao governo norte-americano recolher comunicações de não norte-americanos localizados fora do território nacional sem autorização judicial individual prévia, sem notificação ao afetado e sem um recurso efetivo comparável ao europeu. A Ordem Executiva 12333 amplia essa capacidade de forma análoga fora do território nacional. O tribunal concluiu que o cidadão europeu, perante o sistema jurídico norte-americano, não dispõe da proteção essencialmente equivalente que a Carta exige. A equivalência, portanto, não existe.

Daí a consequência direta: a Decisão 2016/1250 da Comissão Europeia, que tinha validado o Privacy Shield como quadro adequado para as transferências, foi declarada inválida. Toda a transferência amparada unicamente nesse quadro ficou sem base jurídica desde esse mesmo instante.

O que sobreviveu (e sob que condições)

O Schrems II não eliminou todos os instrumentos. As Cláusulas Contratuais-Tipo — as SCC no jargão internacional, pelas suas siglas inglesas Standard Contractual Clauses — sobreviveram. São contratos-tipo aprovados pela Comissão Europeia: um exportador europeu e um importador do país de destino assinam-nos, comprometendo-se a tratar os dados segundo o padrão europeu. A empresa que pensou ter resolvido o problema no dia 17 de julho de 2020 assinou SCC com o seu fornecedor e deu-se por satisfeita.

O desconforto surgiu ao ler a sentença com atenção. O tribunal deixou claro que as SCC continuam a ser válidas, mas a sua validade depende de uma condição que convém sublinhar: que o importador do dado as possa cumprir na prática. Se a legislação nacional do país de destino o impede de cumprir as cláusulas — porque, por exemplo, uma ordem sob a FISA 702 o obriga a entregar os dados sem notificar a sua contraparte europeia —, as cláusulas não protegem na realidade. E então, diz o tribunal, o exportador europeu deve suspender a transferência.

Isto introduziu um novo objeto na prática europeia de proteção de dados: a Transfer Impact Assessment, ou análise de impacto da transferência, conhecida pela sua sigla inglesa TIA. Cada vez que uma empresa europeia quer transferir dados para os Estados Unidos ao abrigo de SCC, deve avaliar formalmente se o destinatário pode cumprir as cláusulas dada a legislação que lhe é aplicável. O Comité Europeu para a Proteção de Dados publicou orientações detalhadas sobre como conduzir a TIA. A prática honesta costuma dar o mesmo resultado: se o importador for uma filial norte-americana de um gigante da cloud, a resposta sincera à TIA é que as cláusulas não podem ser cumpridas tal como estão escritas.

O Privacy Framework e o Schrems III pendente

Em 10 de julho de 2023, a Comissão Europeia adotou uma nova Decisão de Adequação: a 2023/1795. Substitui o extinto Privacy Shield e opera sob o nome EU-US Data Privacy Framework. Os Estados Unidos modificaram previamente o seu regime interno através da Ordem Executiva 14086, que limita o alcance da inteligência de sinais ao «necessário e proporcionado» — terminologia familiar para o leitor europeu, nem tanto para a prática administrativa norte-americana — e cria um órgão de revisão chamado Data Protection Review Court (DPRC). A Comissão considerou que estas modificações eram suficientes para restabelecer o nível essencialmente equivalente.

A organização noyb, fundada por Schrems, interpôs uma denúncia em 7 de setembro de 2023 contra a nova Decisão. Os argumentos são os esperados: o DPRC não é um tribunal independente no sentido do artigo 47 da Carta; os conceitos «necessário e proporcionado» não traduzem mecanicamente os padrões europeus; e, finalmente, uma proteção que assenta numa Ordem Executiva pode ser revogada pela Ordem Executiva seguinte. Uma sentença do TJUE sobre a nova Decisão — a que muitos já chamam, com certa resignação, Schrems III — é esperada para os próximos anos. O resultado não pode ser antecipado. A estrutura do argumento, em qualquer caso, recorda muito a de 2020.

O que a PME europeia não ouve

Enquanto a grande sala do TJUE delibera, a sociedade de advogados de média dimensão continua a trocar correspondência com os seus clientes através do Microsoft 365 alojado em regiões europeias, mas propriedade de uma empresa norte-americana sujeita à FISA 702. A consulta médica privada sincroniza agendas através do Google Workspace. O consultor fiscal envia declarações assinadas através do DocuSign. O psicólogo fatura a partir de uma folha de cálculo no Notion. O escritório de advogados laboralistas arquiva processos no Dropbox. E praticamente todos eles, além disso, atendem os seus clientes pelo WhatsApp. Tudo isto pode operar

amparado, segundo os fornecedores, na Decisão de Adequação 2023/1795. O dia em que essa Decisão cair no Schrems III, todas essas relações ficam desprotegidas no mesmo segundo.

A questão não é retórica. Entre 2022 e 2024, várias autoridades europeias resolveram processos contra responsáveis pelo tratamento por usarem o Google Analytics sem instrumento adequado de transferência, em aplicação literal do raciocínio do TJUE mesmo antes de o Privacy Framework entrar em vigor. A autoridade francesa, a CNIL, foi a primeira a formalizar o critério em 2022; as autoridades austríaca, italiana e outras seguiram-se pouco depois. O incumprimento, sob o atual desenho operacional da PME europeia, documenta-se em tempo real perante quem souber olhar.

A TIA como instrumento, não como ritual

Uma parte considerável das TIA que circulam por escritórios europeus são, lidas com atenção, exercícios formais. Listam os instrumentos contratuais, enumeram as certificações do fornecedor, citam as garantias técnicas, marcam a casa. Poucas se perguntam seriamente se uma ordem FISA 702 obrigaria o fornecedor a entregar os dados. Ainda menos se perguntam o que aconteceria com essa transferência sob uma hipotética revisão do Privacy Framework. O artigo 5 do RGPD exige que o responsável pelo tratamento seja capaz de demonstrar o cumprimento. Uma TIA que não é feita seriamente não demonstra nada; o que demonstra é a vontade de cumprir no papel enquanto se faz o contrário na prática.

A versão sincera da TIA começa com uma pergunta simples: o que aconteceria se amanhã chegasse a este fornecedor uma ordem FISA 702 sobre estes dados concretos? Se a resposta honesta for «teria de os entregar sem nos avisar», as cláusulas contratuais não resolvem o problema. O que resolve, nos casos em que a pergunta importa de verdade, é não ter colocado o dado nas mãos desse fornecedor.

A mudança política como risco estrutural

Há uma camada adicional, política, que convém nomear sem dramatismo. A Decisão de Adequação 2023/1795 assenta, em última análise, na Ordem Executiva 14086, assinada pelo presidente Biden em outubro de 2022. Uma Ordem Executiva é assinada por um presidente e pode ser revogada, modificada ou esvaziada de conteúdo pelo seguinte. A proteção dos dados europeus nos Estados Unidos depende, assim, de uma decisão administrativa que nem o Congresso americano garante nem o sistema jurídico americano protege com a solidez com que protege outras matérias internas. Desde janeiro de 2025, uma nova administração governa os Estados Unidos, e a pergunta sobre a continuidade prática da EO 14086 deixou de ser uma hipótese para se tornar contemporânea. Qualquer cenário em que a administração decida retirar ou atenuar a Ordem deixaria a Decisão Europeia sem a peça sobre a qual foi construída.

Não é um argumento conspiratório. É a leitura sóbria do desenho jurídico. Os quadros de proteção de dados transatlânticos já caíram duas vezes: o Safe Harbor em 2015 (sentença Schrems I), o Privacy Shield em 2020 (Schrems II). O terceiro assenta numa peça mais frágil do que os seus dois antecessores. Uma empresa europeia que aposta hoje o seu tratamento de dados nessa peça está a tomar uma decisão de gestão de risco, não de mero cumprimento normativo.

Para o leitor profissional

As perguntas operacionais que convém formular antes de escolher um serviço cloud para dados profissionais — com o rigor com que um inspetor de proteção de dados as colocaria — são as seguintes:

1. Onde são armazenados fisicamente os dados? Uma região europeia não é resposta suficiente se o operador for norte-americano.
2. Quem opera o serviço, em que jurisdição está incorporado e a que ordens legais pode ser submetido?

3. Que instrumento de transferência é invocado: Decisão de Adequação 2023/1795, SCC com TIA, derrogação do artigo 49 do RGPD? Essa escolha é defensável perante uma inspeção?
4. Se a Decisão de Adequação caísse amanhã, que plano operacional existe para manter a atividade?
5. Existe uma alternativa europeia ou auto-hospedada para essa função e qual seria o custo real da migração?

Nem todas as funções do quotidiano exigem a mesma resposta. Uma folha de cálculo para contabilidade interna provavelmente não eleva a pergunta a este nível. O processo penal de um cliente, o historial clínico, a folha de pagamentos dos funcionários, sim. A proporcionalidade é legítima; a inércia coletiva com que a PME europeia permaneceu em fornecedores norte-americanos para tudo — inclusive para o mais sensível — não o é.

O Schrems II completa seis anos este julho. A sentença não mudou os hábitos quotidianos da maioria das empresas europeas. Mudou, sim, o mapa de riscos a que essas empresas estão expostas. Quando uma decisão administrativa norte-americana se interpõe entre o regulamento europeu e a operacionalidade real de uma PME, convém pelo menos saber que a decisão existe e que é frágil. Aqueles de nós que escolheram uma arquitetura sem operador pelo meio — o fio que percorre a Cuadernos Lacre — prefeririam não ter de escrever este tipo de análise cada vez que um Schrems decide apresentar um recurso. Mas continuaremos a fazê-lo.

Fontes e leitura adicional

- Tribunal de Justiça da União Europeia — sentença de 16 de julho de 2020, processo C-311/18, *Data Protection Commissioner contra Facebook Ireland Ltd. e Maximillian Schrems*.
- Regulamento (UE) 2016/679, capítulo V, artigos 44 a 50 — transferências internacionais de dados pessoais.
- Decisão de Execução (UE) 2023/1795 da Comissão, de 10 de julho de 2023, sobre o nível adequado de proteção dos dados pessoais no âmbito do EU-US Data Privacy Framework.
- Comité Europeu para a Proteção de Dados — *Recomendações 01/2020 sobre as medidas que complementam os instrumentos de transferência para garantir o cumprimento do nível de proteção de dados pessoais da UE*, adotadas em 18 de junho de 2021.
- noyb.eu — denúncia interposta em 7 de setembro de 2023 contra a Decisão (UE) 2023/1795 perante as autoridades europeias de proteção de dados.
- *Foreign Intelligence Surveillance Act*, secção 702 (codificada em 50 U.S.C. § 1881a), e Ordem Executiva 12333 sobre atividades de inteligência norte-americana fora do território nacional.

← AnteriorQuando não há ninguém no meioSeguinte →O que é realmente o SHA-256

Leituras recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Leve este artigo para onde precisar.

↓ Markdown ↓ Texto simples ↓ PDF

O arquivo é descarregado no seu dispositivo. A partir daí, pode guardá-lo, importá-lo no Solo2 ou partilhá-lo onde quiser. Cuadernos não decide o destino por si.

Selo de lacre · SHA-256 a803808d0736478b4fedaee6efabfaeffb6b49f23bc4c8d613887a7d238b6cfb

Cuadernos Lacre · Uma publicação da Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada pela equipa do Solo2.

Este site não utiliza cookies e não carrega recursos de terceiros. Utiliza um contador anónimo de visitas alojado por nós (Umami, no nosso servidor europeu) e o mínimo de JavaScript necessário para a sua preferência de tema claro/escuro. Sem trackers, sem perfilagem, sem partilha de dados. Se quiser seguir-nos: RSS.