

Schrems II، بعد خمس سنوات

الحكم الذي غير قانون نقل البيانات الشخصية الدولية. بعد مرور خمس سنوات، لا يزال جزء كبير من العمل اليومي للمكاتب الأوروبية يعمل وكأن شيئاً لم يكن.

الحكمة التي استغرقت ثلاث ساعات لتغيير القواعد

في 16 يوليو 2020، حوالي الساعة العاشرة والربع صباحاً بتوقيت لوكسمبورغ، أصدرت محكمة العدل للاتحاد الأوروبي (TJUE) حكمها في القضية C-311/18. وفي الساعات الثلاث التالية، توقف النظام القانوني الذي كان يدعم النقل اليومي للبيانات الشخصية من أوروبا إلى الولايات المتحدة — ما يسمى بـ Privacy Shield في تسميته الرسمية — عن الوجود. وبحلول الوقت الذي انتهى فيه مسؤولو حماية البيانات الأوروبيون من غدائهم في ذلك اليوم، لم يعد الإطار الذي كانت تعمل بموجبه شركاتهم وإداراتهم صالحاً.

يُعرف الحكم اليوم باسم Schrems II، تيمناً بماكسيميليان شريمز، الناشط النمساوي الذي أطلق شرارة الدعوى ضد فيسبوك أيرلندا. تناولت الدعوى، بشكل ملموس، عمليات النقل بين فيسبوك أيرلندا وفيسبوك الولايات المتحدة. أما الحكم، بشكل عام، فقد ذهب إلى أبعد من ذلك بكثير: حيث يحدد كيف وتحت أي شروط يمكن نقل أي بيانات شخصية يتم جمعها في الأراضي الأوروبية إلى الولايات المتحدة.

بعد ست سنوات تقريباً، أصبح إطار العمل البديل موجوداً — EU-US Data Privacy Framework، الذي اعتمد في يوليو 2023 — وهو يخضع أيضاً لضغوط قانونية. جولة Schrems جديدة قيد التحضير. وفي الوقت نفسه، لا تزال الشركات الصغيرة والمتوسطة الأوروبية تستخدم خدمات السحاب الأمريكية للمهام اليومية، في معظمها دون أن تدرك أن المسألة القانونية التي تستند إليها تلك الخدمات لا تزال مفتوحة.

ماذا قال Schrems II بالضبط

يستند الحكم إلى ثلاث قطع. الأولى هي ميثاق الحقوق الأساسية للاتحاد الأوروبي، ولا سيما المادتان 7 (الحياة الخاصة والعائلية) و 8 (حماية البيانات الشخصية) والمادة 47 (الحماية القضائية الفعالة). والثانية هي اللائحة العامة لحماية البيانات (RGPD) — التي لا يتذكرها الكثير من الأوروبيين إلا من خلال إشعارات ملفات تعريف الارتباط — وتحديداً الفصل الخامس، المواد 44 إلى 50 (art. 44 to 50)، بشأن عمليات النقل الدولية. والثالثة هي تشريعات الاستخبارات الأمريكية: القسم 702 من قانون مراقبة الاستخبارات الأجنبية، FISA 702 في الاصطلاح القانوني، والأمر التنفيذي الرئاسي 12333.

شرعت المحكمة في المقارنة. يتطلب ميثاق الحقوق الأساسية أن تتمتع البيانات الشخصية للمواطنين الأوروبيين، عندما تغادر الاتحاد، بمستوى من الحماية يعادل جوهرياً المستوى الذي يضمنه RGPD. وبالتالي، كان السؤال هو ما إذا كانت الولايات المتحدة تقدم هذا المستوى المعادل جوهرياً.

كانت الإجابة سلبية، وليس بسبب التفاصيل. تسمح المادة 702 FISA للحكومة الأمريكية بجمع اتصالات غير الأمريكيين المقيمين خارج الأراضي الوطنية دون إذن قضائي فردي مسبق، ودون إخطار المتضرر، ودون وسيلة انتصاف فعالة مماثلة للوسيلة الأوروبية. ويوسع الأمر التنفيذي 12333 هذه القدرة بشكل مماثل خارج الأراضي الوطنية. وخلصت المحكمة إلى أن المواطن الأوروبي، أمام النظام القانوني الأمريكي، لا يتمتع بالحماية المعادلة جوهرياً التي يتطلبها الميثاق. وبالتالي، فإن التكافؤ غير موجود.

ومن هنا جاءت النتيجة المباشرة: أعلن بطلان قرار المفوضية الأوروبية 2016/1250، الذي كان قد صادق على Privacy Shield كإطار ملائم لعمليات النقل. وبقي كل نقل يعتمد حصرياً على ذلك الإطار بدون أساس قانوني منذ تلك اللحظة بالذات.

ما الذي نجا (وتحت أي شروط)

لم يبلغ Schrems II جميع الأدوات. فقد نجت البنود التعاقدية القياسية — SCC في الاصطلاح الدولي، باختصارها الإنجليزي Standard Contractual Clauses. وهي عقود نموذجية معتمدة من قبل المفوضية الأوروبية: حيث يوقع عليها مصدر أوروبي ومستورد من بلد المقصد، ملتزمين بمعالجة البيانات وفقاً للمعايير الأوروبية. اعتقدت الشركة التي اعتقدت أنها حلت المشكلة في 17 يوليو 2020 أنها وقعت SCC مع مزودها واكتفت بذلك.

جاء عدم الارتياح عند قراءة الحكم ببطء. أوضحت المحكمة أن SCC لا تزال صالحة، لكن صلاحيتها تعتمد على شرط يجدر التأكيد عليه: وهو أن يتمكن مستورد البيانات من الوفاء بها في الممارسة العملية. إذا كان التشريع الوطني لبلد المقصد يمنعه من الامتثال للبنود — لأن أمراً بموجب FISA 702، على سبيل المثال، يجبره على تسليم البيانات دون إخطار نظيره الأوروبي — فإن البنود لا تحمي في الواقع. وعندئذ، تقول المحكمة، يجب على المصدر الأوروبي تعليق النقل.

أدى ذلك إلى إدخال عنصر جديد في ممارسة حماية البيانات الأوروبية: تقييم تأثير النقل، المعروف باختصاره الإنجليزي TIA. في كل مرة ترغب فيها شركة أوروبية في نقل البيانات إلى الولايات المتحدة بموجب SCC، يجب عليها تقييم ما إذا كان المستلم قادراً على الالتزام بالبنود نظراً للتشريعات المطبقة عليه بشكل رسمي. نشر المجلس الأوروبي لحماية البيانات (EDPB) إرشادات مفصلة حول كيفية إجراء TIA. وعادة ما تؤدي الممارسة النزيهة إلى نفس النتيجة: إذا كان المستورد شركة أمريكية تابعة لإحدى شركات السحاب الكبرى، فإن الإجابة الصادقة على TIA هي أنه لا يمكن الالتزام بالبنود كما هي مكتوبة.

Privacy Framework و Schrems III المعلق

في 10 يوليو 2023، اعتمدت المفوضية الأوروبية قرار ملاءمة جديداً: 2023/1795. وهو يحل محل Privacy Shield الراحل ويعمل تحت اسم EU-US Data Privacy Framework. عدلت الولايات المتحدة سابقاً نظامها الداخلي بموجب الأمر التنفيذي 14086، الذي يقصر نطاق استخبارات الإشارات على ما هو «ضروري ومتناسب» — وهي مصطلحات مألوفة للقارئ الأوروبي، ولكن ليس كثيراً للممارسة الإدارية الأمريكية — وينشئ هيئة مراجعة تسمى محكمة مراجعة حماية البيانات (DPRC). اعتبرت المفوضية أن هذه التعديلات كافية لاستعادة مستوى معادل جوهرياً.

رفعت منظمة noyb، التي أسسها Schrems، دعوى في 7 سبتمبر 2023 ضد القرار الجديد. الحجج هي ما كان متوقعاً: DPRC ليست محكمة مستقلة بالمعنى المقصود في المادة 47 (art. 47) من الميثاق؛ ومفاهيم «الضرورة والتناسب» لا تترجم المعايير الأوروبية بشكل آلي؛ وأخيراً، يمكن إلغاء الحماية التي تستند إلى أمر تنفيذي بموجب الأمر التنفيذي التالي. من المتوقع صدور حكم من TJUE بشأن القرار الجديد — الذي يسميه الكثيرون بالفعل، بشيء من الاستسلام، Schrems III — في السنوات القادمة. لا يمكن توقع النتيجة. وبأي حال، فإن هيكل الحجة يذكرنا كثيراً بهيكل عام 2020.

ما لا تسمعه الشركات الصغيرة والمتوسطة الأوروبية

بينما تتداول الغرفة الكبرى في TJUE، لا تزال مكاتب المحاماة متوسطة الحجم تتبادل المراسلات مع عملائها من خلال Microsoft 365 المستضاف في المناطق الأوروبية ولكن المملوك لشركة أمريكية تخضع للمادة 702 (FISA 702). وتقوم العيادات الطبية الخاصة بمزامنة جداول الأعمال من خلال Google Workspace. ويرسل المستشار الضريبي الإقرارات الموقعة عبر DocuSign. ويقوم الأخصائي النفسي بإصدار الفواتير من جدول بيانات في Notion. ويقوم مكتب العمل بأرشفة الملفات في Dropbox. وتقريباً جميعهم، بالإضافة إلى ذلك، يتواصلون مع عملائهم عبر WhatsApp. كل هذا يمكن أن يعمل بموجب قرار الملاءمة 2023/1795، وفقاً للمزودين. في اليوم الذي يسقط فيه هذا القرار في Schrems III، ستظل كل هذه العلاقات في العراء في نفس اللحظة.

المسألة ليست بلاغية. بين عامي 2022 و 2024، قامت العديد من السلطات الأوروبية بتسوية ملفات ضد مسؤولي المعالجة لاستخدامهم Google Analytics دون أداة نقل مناسبة، في تطبيق حرفي لمنطق TJUE حتى قبل دخول Privacy Framework حيز التنفيذ. وكانت السلطة الفرنسية، CNIL، أول من صاغ المعيار رسمياً في عام 2022؛ وتبعتها السلطات النمساوية والإيطالية وغيرها بعد ذلك بوقت قصير. إن عدم الامتثال، في ظل التصميم التشغيلي الحالي للشركات الصغيرة والمتوسطة الأوروبية، يتم توثيقه في الوقت الفعلي أمام كل من يعرف كيف ينظر.

TIA كأداة وليس كطقوس

إن جزءاً كبيراً من الـ TIA المتداولة في المكاتب الأوروبية هي، عند قراءتها بعناية، تمارين شكلية. فهي تسرد الأدوات التعاقدية، وتعدد شهادات المزود، وتستشهد بالضمانات التقنية، وتضع علامة في الخانة. قلة منها تتساءل بجدية عما إذا كان أمر FISA 702 سيغير المزود على تسليم البيانات. والأقل من ذلك يتساءلون عما سيحدث لهذا النقل في ظل مراجعة افتراضية لـ Privacy Framework. تتطلب المادة 5 (art. 5) من RGPD من مسؤول المعالجة أن يكون قادراً على إثبات الامتثال. إن TIA التي لا تؤخذ على محمل الجد لا تثبت شيئاً؛ ما تثبتته هو الرغبة في الامتثال على الورق مع القيام بالعكس في الممارسة العملية.

تبدأ النسخة الصادقة من TIA بسؤال بسيط: ماذا سيحدث إذا تلقى هذا المزود غداً أمراً بموجب FISA 702 بشأن هذه البيانات المحددة؟ إذا كانت الإجابة الصادقة هي «سيتعين عليه تسليمها دون إخطارنا»، فإن البنود التعاقدية لا تحل المشكلة. ما يحلها، في الحالات التي يكون فيها السؤال مهماً حقاً، هو عدم وضع البيانات في يد ذلك المزود.

التغيير السياسي كخطر هيكلية

هناك طبقة إضافية، سياسية، يجدر تسميتها دون دراما. يعتمد قرار الملاءمة 2023/1795، في نهاية المطاف، على الأمر التنفيذي 14086، الذي وقعه الرئيس بايدن في أكتوبر 2022. يوقع الرئيس على أمر تنفيذي، ويمكن للرئيس التالي إلغاؤه أو تعديله أو إفراغه من محتواه. وبالتالي، فإن حماية البيانات الأوروبية في الولايات المتحدة تعتمد على قرار إداري لا يضمنه الكونغرس الأمريكي ولا يحميه النظام القانوني الأمريكي بنفس القوة التي يحمي بها المسائل الداخلية الأخرى. منذ يناير 2025، تدير إدارة جديدة الولايات المتحدة، ولم يعد السؤال عن الاستمرارية العملية للأمر التنفيذي 14086 فرضية بل أصبح معاصراً. إن أي سيناريو تقرر فيه الإدارة سحب أو تخفيف الأمر سيترك القرار الأوروبي بدون القطعة التي بُني عليها.

هذه ليست حجة تأمرية. إنها قراءة رصينة للتصميم القانوني. لقد سقطت أطر حماية البيانات عبر الأطلسي مرتين بالفعل: Safe Harbor في عام 2015 (حكم Schrems I)، و Privacy Shield في عام 2020 (Schrems II). والثالث يعتمد على قطعة أكثر هشاشة من سابقتها. إن الشركة الأوروبية التي تراهن اليوم بمعالجة بياناتها على تلك القطعة تتخذ قراراً بإدارة المخاطر، وليس مجرد امتثال تنظيمي.

للقارئ المهني

الأسئلة التشغيلية التي يجب طرحها قبل اختيار خدمة سحابية للبيانات المهنية — بالصرامة التي يطرحها مفتش حماية البيانات — هي كما يلي:

1. أين يتم تخزين البيانات مادياً؟ لا تكفي المنطقة الأوروبية كإجابة إذا كان المشغل أمريكياً.
2. من يدير الخدمة، وفي أي ولاية قضائية تم تأسيسها، وما هي الأوامر القانونية التي يمكن أن تخضع لها؟
3. ما هي أداة النقل التي يتم الاستناد إليها: قرار الملاءمة 2023/1795، أو SCC مع TIA، أو الاستثناء من المادة 49 (art. 49) من RGPD؟ هل يمكن الدفاع عن هذا الاختيار أمام التفتيش؟
4. إذا سقط قرار الملاءمة غداً، فما هي الخطة التشغيلية الموجودة للحفاظ على النشاط؟
5. هل هناك بديل أوروبي أو استضافة ذاتية لهذه الوظيفة، وما هي التكلفة الحقيقية للهجرة؟

لا تتطلب جميع وظائف المكتب اليومية نفس الاستجابة. فجدول بيانات للمحاسبة الداخلية ربما لا يرفع السؤال إلى هذا المستوى. لكن السجل الجنائي للعمليات، والتاريخ الطبي، وكشوف رواتب الموظفين، تتطلب ذلك. التناسب مشروع؛ أما القصور الذاتي الجماعي الذي طلت الشركات الصغيرة والمتوسطة الأوروبية بموجبه تعتمد على مزودين أمريكيين في كل شيء — حتى في أكثر الأمور حساسية — فهو ليس كذلك.

يصادف شهر يوليو الجاري مرور ست سنوات على صدور حكم Schrems II. لم تغير هذه السنتنتية العادات اليومية لغالبية الشركات الأوروبية. ولكنها غيرت خريطة المخاطر التي تتعرض لها تلك الشركات. عندما يقف قرار إداري أمريكي عائقاً بين اللوائح الأوروبية والعمليات الواقعية لشركة صغيرة أو متوسطة، فمن الأفضل على الأقل معرفة أن هذا القرار موجود، وأنه هش. نحن الذين اخترنا هندسة معمارية بدون وسيط — الخيط الذي يمر عبر Cuadernos Lacre — نفضل ألا نضطر إلى كتابة هذا النوع من التحليلات في كل مرة يقرر فيها Schrems تقديم استئناف. لكننا سنواصل القيام بذلك.

المصادر ومزيد من القراءة

- محكمة العدل للاتحاد الأوروبي (TJUE) — حكم الصادر في 16 يوليو 2020، القضية C-311/18، مفوض حماية البيانات ضد شركة فيسبوك أيرلندا المحدودة وماكسيميليان شريمز.
- اللائحة (UE) 2016/679، الفصل الخامس، المواد 44 إلى 50 — عمليات النقل الدولي للبيانات الشخصية.
- قرار التنفيذ (UE) 2023/1795 الصادر عن المفوضية، بتاريخ 10 يوليو 2023، بشأن المستوى المناسب لحماية البيانات الشخصية في إطار EU-US Data Privacy Framework.
- المجلس الأوروبي لحماية البيانات (EDPB) — التوصيات 01/2020 بشأن التدابير التي تكمل أدوات النقل لضمان الامتثال لمستوى حماية البيانات الشخصية في الاتحاد الأوروبي، المعتمدة في 18 يونيو 2021.
- noyb.eu — دعوى مرفوعة في 7 سبتمبر 2023 ضد القرار (UE) 2023/1795 أمام السلطات الأوروبية لحماية البيانات.
- Foreign Intelligence Surveillance Act، القسم 702 (الرمز في U.S.C. § 1881a 50)، والأمر التنفيذي 12333 بشأن أنشطة الاستخبارات الأمريكية خارج الأراضي الوطنية.

← [السابق عندما لا يوجد أحد في المنتصف التالي](#) → [CUADERNOS LIST SHA256 TITLE](#)

قراءات حديثة

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

خذ هذا المقال معك أينما احتجت إليه.

↓ [ماركداون](#) ↓ [نص عادي](#) ↓ [PDF](#)

سيتم تنزيل الملف على جهازك. من هناك يمكنك حفظه، أو استيراده إلى Solo2 أو مشاركته أينما تريد. Cuadernos لا تقرر الوجهة نيابة عنك.

ختم شمعي · SHA-256 99f92cbaab7a866f3383309b01d2d744d8e4049bf913e89eachf468d9a5f26d4

- [Cuadernos Lacre](#) · منشور لشركة [Menzuri Gestión S.L.](#)
- بقلم R.Eugenio · تحرير فريق [Solo2](#).

هذا الموقع لا يستخدم ملفات تعريف الارتباط (cookies) ولا يحمل موارد من أطراف ثالثة. يستخدم عداد زيارات مجهول مستضاف ذاتياً (Umami، على خادمنا الأوروبي) والحد الأدنى من JavaScript اللازم لتفضيل المظهر الفاتح/الداكن. لا يوجد متابعون، لا يوجد تصنيف، لا توجد مشاركة بيانات. إذا كنت ترغب في متابعتنا: [RSS](#).