شرمز ۲، پنج سال بعد

حکمی که قانون انتقال بین‌المللی داده‌های شخصی را تغییر داد. پنج سال بعد، بخش قابل توجهی از فعالیت‌های روزمره دفاتر اروپایی همچنان طوری عمل می‌کنند که گویی هیچ اتفاقی نیفتاده است.

برای اینکه متوجه شویم: در ۱۶ ژوئیه ۲۰۲۰، در یک صبح پنجشنبه، یک دادگاه اروپایی بخش بزرگی از نحوه ارسال داده‌های شما توسط شرکت‌ها به ایالات متحده را غیرقانونی اعلام کرد. پنج سال بعد، تقریباً هیچ‌کس چیزی را تغییر نداده است. اطلاعات شما دقیقاً مانند آن زمان به پرواز خود ادامه می‌دهد.

حکمی که در سه ساعت قوانین را تغییر داد

در ۱۶ جولای ۲۰۲۰، حوالی ساعت ده و ربع صبح به وقت لوکزامبورگ، دیوان دادگستری اتحادیه اروپا (TJUE) حکم پرونده C-311/18 را منتشر کرد. در سه ساعت بعد، رژیم حقوقی که انتقال روزانه داده‌های شخصی از اروپا به ایالات متحده را پشتیبانی می‌کرد —موسوم به Privacy Shield (سپر حریم خصوصی)— از هستی ساقط شد. وقتی مسئولان حفاظت از داده‌های اروپایی ناهار آن روز را تمام کردند، چارچوبی که شرکت‌ها و ادارات آن‌ها تحت آن فعالیت می‌کردند، دیگر کارایی نداشت.

این حکم امروزه با نام شرمز ۲ شناخته می‌شود، به افتخار ماکسیمیلیان شرمز، فعال اتریشی که شکایتش علیه فیس‌بوک ایرلند آن را به جریان انداخت. شکایت در جزئیات به انتقال داده‌ها بین فیس‌بوک ایرلند و فیس‌بوک ایالات متحده می‌پرداخت. حکم در کلیات بسیار فراتر می‌رود: تعیین می‌کند که هر داده شخصی جمع‌آوری شده در خاک اروپا، چگونه و تحت چه شرایطی می‌تواند به ایالات متحده منتقل شود.

تقریباً شش سال بعد، چارچوب جایگزین وجود دارد —EU-US Data Privacy Framework که در جولای ۲۰۲۳ پذیرفته شد— و آن نیز تحت فشار حقوقی است. دور جدیدی از پرونده‌های شرمز در حال آماده‌سازی است. در این میان، شرکت‌های کوچک و متوسط اروپایی همچنان از خدمات ابری ایالات متحده برای کارهای روزمره استفاده می‌کنند، که اکثر آن‌ها نمی‌دانند مسئله حقوقی که این خدمات بر آن استوارند همچنان باز است.

شرمز ۲ دقیقاً چه می‌گفت

حکم بر سه قطعه استوار است. اولی منشور حقوق اساسی اتحادیه اروپا، به ویژه مواد ۷ (زندگی خصوصی و خانوادگی)، ۸ (حفاظت از داده‌های شخصی) و ۴۷ (حمایت قضایی موثر) است. دومی مقررات عمومی حفاظت از داده‌ها —همان RGPD که بسیاری از اروپایی‌ها فقط به خاطر هشدارهای کوکی آن را به یاد می‌آورند—، به ویژه فصل پنجم آن، مواد ۴۴ تا ۵۰ در مورد انتقال بین‌المللی است. سومی قوانین اطلاعاتی ایالات متحده است: بخش ۷۰۲ قانون نظارت بر اطلاعات خارجی یا FISA 702 در اصطلاح حقوقی، و فرمان اجرایی ریاست جمهوری ۱۲۳۳۳.

دادگاه از طریق مقایسه عمل کرد. منشور حقوق اساسی ایجاب می‌کند که داده‌های شخصی شهروندان اروپایی هنگام خروج از اتحادیه، از سطح حفاظتی «اساساً معادل» با آنچه توسط RGPD تضمین شده، برخوردار باشند. سوال در نتیجه این بود که آیا ایالات متحده چنین سطح اساساً معادلی را ارائه می‌دهد یا خیر.

پاسخ منفی بود و این به خاطر جزئیات نبود. FISA 702 به دولت آمریکا اجازه می‌دهد ارتباطات غیرآمریکایی‌های مقیم خارج از قلمرو ملی را بدون اجازه قضایی انفرادی قبلی، بدون اطلاع به فرد آسیب‌دیده و بدون یک منبع موثر قابل مقایسه با اروپا جمع‌آوری کند. فرمان اجرایی ۱۲۳۳۳ این توانایی را به شکلی مشابه در خارج از قلمرو ملی

گسترش می‌دهد. دادگاه به این نتیجه رسید که شهروند اروپایی در برابر سیستم حقوقی ایالات متحده، از حفاظت اساساً معادلی که منشور ایجاب می‌کند برخوردار نیست. بنابراین، معادل بودن وجود ندارد.

از اینجا نتیجه مستقیم حاصل شد: تصمیم ۲۰۱۶/۱۲۵۰ کمیسیون اروپا که Privacy Shield را به عنوان چارچوب مناسب برای انتقال‌ها تایید کرده بود، فاقد اعتبار اعلام شد. تمام انتقال‌هایی که تنها بر آن چارچوب استوار بودند، از همان لحظه بدون پایه حقوقی ماندند.

آنچه باقی ماند (و تحت چه شرایطی)

شرمز ۲ تمام ابزارها را حذف نکرد. مفاد قراردادی استاندارد —SCC در اصطلاح بین‌المللی— باقی ماندند. این‌ها قراردادهای نمونه تایید شده توسط کمیسیون اروپا هستند: یک صادرکننده اروپایی و یک واردکننده در کشور مقصد آن‌ها را امضا می‌کنند و متعهد می‌شوند که با داده‌ها طبق استاندارد اروپایی رفتار کنند. شرکتی که فکر می‌کرد مشکل را در ۱۷ جولای ۲۰۲۰ حل کرده است، SCC را با ارائه‌دهنده خود امضا کرد و راضی شد.

ناراحتی زمانی ایجاد شد که حکم با دقت خوانده شد. دادگاه روشن کرد که SCCها همچنان معتبر هستند، اما اعتبار آن‌ها به شرطی بستگی دارد که شایسته است بر آن تأکید شود: اینکه واردکننده داده بتواند در عمل آن‌ها را اجرا کند. اگر قانون ملی کشور مقصد مانع از اجرای مفاد شود —مثلاً به این دلیل که دستوری تحت FISA 702 او را مجبور به تحویل داده‌ها بدون اطلاع به طرف اروپایی کند—، مفاد در واقع محافظتی نمی‌کنند. و در آن صورت، دادگاه می‌گوید صادرکننده اروپایی باید انتقال را متوقف کند.

این امر موضوع جدیدی را به عملکرد حفاظت از داده‌های اروپا وارد کرد: ارزیابی تأثیر انتقال یا Transfer Impact Assessment که با نام اختصاری TIA شناخته می‌شود. هر بار که یک شرکت اروپایی می‌خواهد داده‌ها را تحت پوشش SCC به ایالات متحده منتقل کند، باید رسماً ارزیابی کند که آیا دریافت‌کننده با توجه به قوانینی که بر آن حاکم است، می‌تواند مفاد قرارداد را اجرا کند یا خیر. EDPB دستورالعمل‌های دقیقی درباره نحوه انجام TIA منتشر کرده است. عملکرد صادقانه معمولاً به نتیجه یکسانی ختم می‌شود: اگر واردکننده داده یک شرکت تابعه آمریکایی از غول‌های ابری باشد، پاسخ صادقانه به TIA این است که مفاد قرارداد به شکلی که نوشته شده‌اند، قابل اجرا نیستند.

چارچوب حریم خصوصی و شرمز ۳ در انتظار

در ۱۰ جولای ۲۰۲۳، کمیسیون اروپا تصمیم کفایت جدیدی را اتخاذ کرد: ۲۰۲۳/۱۷۹۵. این تصمیم جایگزین Privacy Shield متوفی شد و تحت عنوان EU-US Data Privacy Framework فعالیت می‌کند. ایالات متحده پیش از آن رژیم داخلی خود را از طریق فرمان اجرایی ۱۴۰۸۶ اصلاح کرد که دامنه سیگنال‌های اطلاعاتی را به موارد «لازم و متناسب» محدود می‌کند —اصطلاحی که برای خواننده اروپایی آشناست اما برای عملکرد اداری آمریکا چندان نه— و نهادی بازنگری به نام Data Protection Review Court (DPRC) ایجاد می‌کند. کمیسیون به این نتیجه رسید که این اصلاحات برای بازگرداندن سطح حفاظتی اساساً معادل کافی است.

سازمان noyb که توسط شرمز تأسیس شده، در ۷ سپتامبر ۲۰۲۳ شکایتی را علیه تصمیم جدید ثبت کرد. استدلال‌ها همان‌طور که انتظار می‌رود هستند: DPRC یک دادگاه مستقل به معنای ماده ۴۷ منشور نیست؛ مفاهیم «لازم و متناسب» استانداردهای اروپایی را به طور خودکار ترجمه نمی‌کنند؛ و در نهایت، حفاظتی که بر پایه یک فرمان اجرایی استوار است، می‌تواند توسط فرمان اجرایی بعدی لغو شود. انتظار می‌رود حکم TJUE در مورد تصمیم جدید —که بسیاری با نوعی تسلیم آن را شرمز ۳ می‌نامند— در سال‌های آینده صادر شود. نتیجه را نمی‌توان پیش‌بینی کرد، اما ساختار استدلال در هر صورت شباهت زیادی به سال ۲۰۲۰ دارد.

آنچه بنگاه‌های کوچک و متوسط اروپایی نمی‌شنوند

در حالی که تالار بزرگ TJUE در حال شور است، یک دفتر حقوقی متوسط همچنان از طریق Microsoft 365 که در مناطق اروپایی میزبانی می‌شود اما متعلق به یک شرکت آمریکایی مشمول FISA 702 است، با مشتریان خود مکاتبه می‌کند. یک مطب پزشکی خصوصی تقویم‌ها را از طریق Google Workspace همگام‌سازی می‌کند. مشاور مالیاتی اظهارنامه‌های امضا شده را از طریق DocuSign ارسال می‌کند. روانشناس فاکتورها را در یک صفحه

گسترده Notion صادر می‌کند. دفتر حقوقی پرونده‌ها را در Dropbox آرشیو می‌کند. و تقریباً همه آن‌ها از طریق WhatsApp به مشتریان خود پاسخ می‌دهند. به گفته ارائه‌دهندگان، همه این‌ها می‌تواند تحت پوشش تصمیم کفایت ۲۰۲۳/۱۷۹۵ فعالیت کند. روزی که این تصمیم در شرمز ۳ لغو شود، تمام این روابط در همان لحظه بی‌دفاع می‌مانند.

مسئله انتزاعی نیست. بین سال‌های ۲۰۲۲ و ۲۰۲۴، چندین مقام اروپایی پرونده‌هایی را علیه مسئولان کنترل داده به دلیل استفاده از Google Analytics بدون ابزار انتقال مناسب حل‌وفصل کردند که در اجرای مستقیم استدلال TJUE حتی پیش از اجرایی شدن Privacy Framework بود. مقام فرانسوی، CNIL، اولین کسی بود که در سال ۲۰۲۲ این معیار را رسمی کرد؛ مقامات اتریشی، ایتالیایی و دیگران اندکی بعد دنبال کردند. عدم انطباق، تحت طراحی عملیاتی فعلی بنگاه‌های کوچک و متوسط اروپایی، برای هر کسی که بداند کجا را نگاه کند، به صورت لحظه‌ای مستند می‌شود.

TIA به عنوان یک ابزار، نه به عنوان یک تشریفات

بخش قابل توجهی از TIAهایی که در دفاتر اروپایی در جریان هستند، اگر با دقت خوانده شوند، تمرین‌هایی صوری‌اند. آن‌ها ابزارهای قراردادی را لیست می‌کنند، گواهینامه‌های ارائه‌دهنده را می‌شمارند، ضمانت‌های فنی را ذکر می‌کنند و تیک مربوطه را می‌زنند. تعداد کمی به طور جدی می‌پرسند که آیا یک دستور FISA 702 ارائه‌دهنده را مجبور به تحویل داده‌ها می‌کند یا خیر. حتی تعداد کمتری می‌پرسند که با یک بازنگری فرضی در Privacy Framework چه بلایی سر آن انتقال می‌آید. ماده ۵ RGPD از مسئول کنترل داده می‌خواهد که قادر به اثبات انطباق باشد. TIAای که جدی انجام نشود، چیزی را ثابت نمی‌کند؛ آنچه ثابت می‌کند، تمایل به انطباق روی کاغذ است در حالی که در عمل خلاف آن انجام می‌شود.

نسخه صادقانه TIA با یک سوال ساده شروع می‌شود: اگر فردا یک دستور FISA 702 در مورد این داده‌های خاص به این ارائه‌دهنده برسد، چه اتفاقی می‌افتد؟ اگر پاسخ صادقانه این است که «آن‌ها مجبورند داده‌ها را بدون اطلاع ما تحویل دهند»، مفاد قراردادی مشکل را حل نمی‌کنند. آنچه مشکل را حل می‌کند، در مواردی که سوال واقعاً مهم است، قرار ندادن داده‌ها در دست آن ارائه‌دهنده است.

تغییر سیاسی به عنوان یک ریسک ساختاری

یک لایه اضافی، سیاسی، وجود دارد که شایسته است بدون دراماتیک کردن نام برده شود. تصمیم کفایت ۲۰۲۳/۱۷۹۵ در نهایت بر پایه فرمان اجرایی ۱۴۰۸۶ استوار است که توسط رئیس‌جمهور بایدن در اکتبر ۲۰۲۲ امضا شد. یک فرمان اجرایی توسط یک رئیس‌جمهور امضا می‌شود و می‌تواند توسط رئیس‌جمهور بعدی لغو، اصلاح یا از محتوا تهی شود. به این ترتیب، حفاظت از داده‌های اروپایی در ایالات متحده به یک تصمیم اداری وابسته است که نه کنگره آمریکا آن را تضمین می‌کند و نه سیستم حقوقی آمریکا با همان صلابتی که از سایر موضوعات داخلی محافظت می‌کند، از آن محافظت می‌نماید. از ژانویه ۲۰۲۵ دولت جدیدی بر ایالات متحده حاکم است و سوال درباره تداوم عملی فرمان اجرایی ۱۴۰۸۶ از یک فرضیه به یک واقعیت معاصر تبدیل شده است. هر سناریویی که در آن دولت تصمیم به لغو یا تضعیف فرمان بگیرد، تصمیم اروپا را بدون قطعه‌ای که بر آن بنا شده بود، رها خواهد کرد.

این یک استدلال توطئه‌آمیز نیست؛ بلکه قرائت متین طراحی حقوقی است. چارچوب‌های حفاظت از داده فرا-آتلانتیک تاکنون دو بار فروپاشیده‌اند: Safe Harbor در سال ۲۰۱۵ (حکم شرمز ۱) و Privacy Shield در سال ۲۰۲۰ (شرمز ۲). سومی بر پایه‌ای شکننده‌تر از دو سلف خود استوار است. یک شرکت اروپایی که امروز پردازش داده‌های خود را روی این قطعه شرط‌بندی می‌کند، در حال اتخاذ یک تصمیم مدیریت ریسک است، نه صرفاً یک تصمیم انطباق با مقررات.

برای خواننده حرفه‌ای

سوالات عملیاتی که شایسته است قبل از انتخاب یک سرویس ابری برای داده‌های حرفه‌ای مطرح شود —با همان دقتی که یک بازرس حفاظت از داده‌ها آن‌ها را مطرح می‌کند— به شرح زیر است:

1. داده‌ها به صورت فیزیکی در کجا ذخیره می‌شوند؟ اگر اپراتور آمریکایی باشد، منطقه اروپایی پاسخ کافی نیست.
2. چه کسی سرویس را مدیریت می‌کند، در کدام حوزه قضایی ثبت شده است و مشمول چه دستورات قانونی می‌تواند باشد؟
3. کدام ابزار انتقال استناد می‌شود: تصمیم کفایت ۲۰۲۳/۱۷۹۵، SCC با TIA، یا استثنای ماده ۴۹ RGPD؟ آیا این انتخاب در برابر بازرسی قابل دفاع است؟
4. اگر تصمیم کفایت فردا لغو شود، چه طرح عملیاتی برای تداوم فعالیت وجود دارد؟
5. آیا جایگزین اروپایی یا خود-میزبانی برای آن عملکرد وجود دارد و هزینه واقعی مهاجرت چقدر خواهد بود؟

همه عملکردهای روزمره دفتر به پاسخ یکسانی نیاز ندارند. یک صفحه گسترده برای حسابداری داخلی احتمالاً سوال را به این سطح نمی‌برد. اما پرونده کیفری یک مشتری، سوابق پزشکی، لیست حقوق کارکنان، چرا. تناسب امری مشروع است؛ اما اینرسی جمعی که با آن بنگاه‌های کوچک و متوسط اروپایی در ارائه‌دهندگان آمریکایی برای همه چیز —حتی حساس‌ترین موارد— باقی مانده‌اند، مشروع نیست.

شرمز ۲ (Schrems II) در جولای امسال شش ساله می‌شود. این حکم عادت‌های روزمره اکثر شرکت‌های اروپایی را تغییر نداده است؛ اما نقشه ریسک‌هایی را که این شرکت‌ها با آن مواجه هستند، تغییر داده است. وقتی یک تصمیم اداری ایالات متحده بین مقررات اروپایی و عملیات واقعی یک بنگاه کوچک و متوسط (SME) قرار می‌گیرد، حداقل باید دانست که آن تصمیم وجود دارد و شکننده است. کسانی از ما که معماری بدون واسطه را انتخاب کرده‌ایم —رشته‌ای که در Cuadernos Lacre دنبال می‌شود— ترجیح می‌دادیم مجبور نباشیم هر بار که یک پرونده شرمز برای ارائه درخواست تجدیدنظر مطرح می‌شود، این نوع تحلیل‌ها را بنویسیم. اما به انجام آن‌ها ادامه خواهیم داد.

یادداشت تحریریه: وقتی این Cuadernos نام شرکت‌ها یا محصولات را می‌برد، برای متهم کردن نیست. کسانی که آن‌ها را می‌سازند کارهایی انجام می‌دهند که میلیون‌ها نفر از آن استفاده کرده و قدردانی می‌کنند. آنچه ما به آن اشاره می‌کنیم ساختاری است — مدل، نه نام تجاری. نام‌های تجاری به عنوان مثال ذکر می‌شوند چون همان‌هایی هستند که خواننده می‌شناسد.

منابع و مطالعه بیشتر

- دیوان دادگستری اتحادیه اروپا — حکم ۱۶ جولای ۲۰۲۰، پرونده C-311/18، *کمیسر حفاظت از داده علیه فیس‌بوک ایرلند و ماکسیمیلیان شرمز*.
- مقررات (UE) 2016/679، فصل پنجم، مواد ۴۴ تا ۵۰ — انتقال بین‌المللی داده‌های شخصی.
- تصمیم اجرایی (UE) 2023/1795 کمیسیون، ۱۰ جولای ۲۰۲۳، در مورد سطح مناسب حفاظت از داده‌های شخصی در چارچوب EU-US Data Privacy Framework.
- کمیته حفاظت از داده‌های اروپا — *توصیه‌های 01/2020 در مورد اقداماتی که ابزارهای انتقال را برای تضمین انطباق با سطح حفاظت از داده‌های شخصی اتحادیه اروپا تکمیل می‌کنند*، پذیرفته شده در ۱۸ ژوئن ۲۰۲۱.
- noyb.eu — شکایت ثبت شده در ۷ سپتامبر ۲۰۲۳ علیه تصمیم (UE) 2023/1795 نزد مقامات اروپایی حفاظت از داده.
- *قانون نظارت بر اطلاعات خارجی*، بخش ۷۰۲ (کدگذاری شده در 50 U.S.C. § 1881a) و فرمان اجرایی ۱۲۳۳۳ در مورد فعالیت‌های اطلاعاتی ایالات متحده در خارج از قلمرو ملی.

← السابقوقتی هیچ‌کس در میان نیستالتالي → SHA-256 واقعاً چیست

قراءات حديثة

- تحلیل ۱۸۰ مه ۲۰۲۶ حریم خصوصی واقعی در مقابل ظاهری: سؤالاتی که باید از خود بپرسید
- تحلیل ۱۸۰ مه ۲۰۲۶ Self-hosting به عنوان یک فعالیت حرفه‌ای
- مفهوم ۱۸۰ مه ۲۰۲۶ ۲۴ کلمه: هویت رمزنگاری شده چیست

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ مارک‌داون ↓ متن ساده ↓ PDF

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعي · SHA-256 7d17c3486e57833d08401b50ba0564cc23f23537b4a683e73300806e6f4dbc48

Cuadernos Lacre · نشريّة من Menzuri Gestión S.L. ·
كتبها R.Eugenio · حرّرها فريق Solo2.