Phân tích · Ngày 18 tháng 5 năm 2026

← Trước·Tiếp theo →

# Schrems II, năm năm sau

Bản án đã thay đổi luật về chuyển giao dữ liệu cá nhân quốc tế. Năm năm sau, một phần đáng kể các công việc văn phòng hằng ngày của châu Âu vẫn hoạt động như thể không có chuyện gì xảy ra.

## Bản án chỉ mất ba giờ để thay đổi các quy tắc

Vào ngày 16 tháng 7 năm 2020, khoảng mười giờ mười lăm phút sáng theo giờ Luxembourg, Tòa án Công lý Liên minh Châu Âu (CJEU) đã công bố bản án cho vụ việc C-311/18. Trong ba giờ tiếp theo, chế độ pháp lý hỗ trợ việc chuyển giao dữ liệu cá nhân hằng ngày từ châu Âu sang Hoa Kỳ —cái gọi là Lá chắn Quyền riêng tư (Privacy Shield)— đã ngừng tồn tại. Khi các nhân viên bảo vệ dữ liệu châu Âu kết thúc bữa trưa ngày hôm đó, khung pháp lý mà các công ty và cơ quan hành chính của họ vận hành đã không còn giá trị.

Bản án ngày nay được gọi là Schrems II, theo tên Maximilian Schrems, nhà hoạt động người Áo mà đơn khiếu nại chống lại Facebook Ireland đã kích hoạt vụ việc. Cụ thể, đơn khiếu nại đề cập đến việc chuyển giao giữa Facebook Ireland và Facebook Hoa Kỳ. Nói chung, bản án đi xa hơn thế nhiều: nó quy định cách thức và điều kiện để bất kỳ dữ liệu cá nhân nào được thu thập trên lãnh thổ châu Âu có thể được chuyển sang Hoa Kỳ.

Gần sáu năm sau, khung pháp lý thay thế đã tồn tại —EU-US Data Privacy Framework, được thông qua vào tháng 7 năm 2023— và nó cũng đang chịu áp lực pháp lý. Một vòng quay Schrems mới đang được chuẩn bị. Trong khi đó, các doanh nghiệp vừa và nhỏ châu Âu vẫn tiếp tục sử dụng các dịch vụ đám mây của Hoa Kỳ cho các công việc hằng ngày, phần lớn mà không biết rằng vấn đề pháp lý làm nền tảng cho các dịch vụ đó vẫn còn bỏ ngỏ.

## Chính xác thì Schrems II đã nói gì

Bản án dựa trên ba mảnh ghép. Thứ nhất là Hiến chương về các quyền cơ bản của Liên minh Châu Âu, đặc biệt là các điều khoản 7 (đời sống riêng tư và gia đình), 8 (bảo vệ dữ liệu cá nhân) và 47 (quyền được bảo vệ tư pháp hiệu quả). Thứ hai là Quy định chung về bảo vệ dữ liệu —GDPR mà nhiều người châu Âu chỉ nhớ qua các thông báo cookie— cụ thể là Chương V, từ điều khoản 44 đến 50, về chuyển giao quốc tế. Thứ ba là luật tình báo của Hoa Kỳ: mục 702 của Foreign Intelligence Surveillance Act, FISA 702 trong thuật ngữ pháp lý, và Sắc lệnh hành pháp 12333 của Tổng thống.

Tòa án đã tiến hành bằng cách đối chiếu. Hiến chương về các quyền cơ bản yêu cầu dữ liệu cá nhân của công dân châu Âu, khi rời khỏi Liên minh, phải được hưởng một mức độ bảo vệ tương đương về cơ bản với mức độ được đảm bảo bởi GDPR. Do đó, câu hỏi là liệu Hoa Kỳ có cung cấp mức độ tương đương về cơ bản đó hay không.

Câu trả lời là phủ định, và không chỉ vì những sắc thái nhỏ. FISA 702 cho phép chính phủ Hoa Kỳ thu thập thông tin liên lạc của những người không phải người Mỹ ở bên ngoài lãnh thổ quốc gia mà không cần sự cho phép tư pháp riêng biệt trước đó, không thông báo cho người bị ảnh hưởng và không có biện pháp khắc phục hiệu quả có thể so sánh với châu Âu. Sắc lệnh hành pháp 12333 mở rộng khả năng đó một cách tương tự ở bên ngoài lãnh thổ quốc gia. Tòa án kết luận rằng công dân châu Âu, trước hệ thống pháp luật Hoa Kỳ, không có được sự bảo vệ tương đương về cơ bản mà Hiến chương yêu cầu. Do đó, sự tương đương không tồn tại.

Từ đó dẫn đến hệ quả trực tiếp: Quyết định 2016/1250 của Ủy ban Châu Âu, vốn đã công nhận Privacy Shield là khung pháp lý phù hợp cho việc chuyển giao, đã bị tuyên bố vô hiệu. Mọi hoạt động chuyển giao chỉ dựa trên khung pháp lý đó đã mất đi cơ sở pháp lý ngay từ thời điểm đó.

## Những gì thực sự còn tồn tại (và dưới những điều kiện nào)

Schrems II không loại bỏ tất cả các công cụ. Các Điều khoản Hợp đồng Tiêu chuẩn —SCC trong thuật ngữ quốc tế, viết tắt của Standard Contractual Clauses— vẫn còn tồn tại. Đó là các hợp đồng mẫu được Ủy ban Châu Âu phê duyệt: một bên xuất khẩu châu Âu và một bên nhập khẩu của quốc gia đích ký kết chúng, cam kết xử lý dữ liệu theo tiêu chuẩn châu Âu. Công ty nào tưởng rằng đã giải quyết được vấn đề vào ngày 17 tháng 7 năm 2020 bằng cách ký SCC với nhà cung cấp của mình thì đã cảm thấy hài lòng.

Sự khó chịu ập đến khi đọc kỹ bản án. Tòa án đã làm rõ rằng các SCC vẫn có giá trị, nhưng giá trị của chúng phụ thuộc vào một điều kiện cần nhấn mạnh: bên nhập khẩu dữ liệu phải có khả năng thực hiện chúng trong thực tế. Nếu luật pháp quốc gia của quốc gia đích ngăn cản họ tuân thủ các điều khoản —ví dụ, một lệnh theo FISA 702 buộc họ phải giao nộp dữ liệu mà không thông báo cho đối tác châu Âu— thì các điều khoản đó thực tế không bảo vệ được gì. Và khi đó, tòa án nói rằng bên xuất khẩu châu Âu phải đình chỉ việc chuyển giao.

Điều này đã đưa một khái niệm mới vào thực tiễn bảo vệ dữ liệu của châu Âu: Transfer Impact Assessment, hay đánh giá tác động chuyển giao, được biết đến qua tên viết tắt tiếng Anh là TIA. Mỗi khi một công ty châu Âu muốn chuyển dữ liệu sang Hoa Kỳ theo các SCC, họ phải đánh giá chính thức xem bên nhận có thể tuân thủ các điều khoản hay không dựa trên luật pháp áp dụng cho họ. Ủy ban Bảo vệ Dữ liệu Châu Âu (EDPB) đã công bố các hướng dẫn chi tiết về cách thực hiện TIA. Thực tế trung thực thường cho cùng một kết quả: nếu bên nhập khẩu là một chi nhánh tại Hoa Kỳ của một gã khổng lồ đám mây, câu trả lời chân thực cho TIA là các điều khoản không thể được thực hiện như chúng được viết.

## Privacy Framework và vụ Schrems III đang chờ xử lý

Vào ngày 10 tháng 7 năm 2023, Ủy ban Châu Âu đã thông qua một Quyết định Tương xứng mới: 2023/1795. Nó thay thế cho Privacy Shield đã không còn hiệu lực và hoạt động dưới tên gọi EU-US Data Privacy Framework. Trước đó, Hoa Kỳ đã sửa đổi chế độ nội bộ của mình thông qua Sắc lệnh hành pháp (Executive Order) 14086, giới hạn phạm vi tình báo tín hiệu ở mức «cần thiết và tương xứng» —thuật ngữ quen thuộc với độc giả châu Âu, nhưng không phổ biến trong thực tiễn hành chính Hoa Kỳ— và tạo ra một cơ quan xem xét gọi là Data Protection Review Court (DPRC). Ủy ban cho rằng những sửa đổi này là đủ để khôi phục mức độ bảo vệ tương đương về cơ bản.

Tổ chức noyb, do Schrems sáng lập, đã đệ đơn kiện vào ngày 7 tháng 9 năm 2023 chống lại Quyết định mới. Các lập luận đều nằm trong dự đoán: DPRC không phải là một tòa án độc lập theo ý nghĩa của điều khoản 47 trong Hiến chương; các khái niệm «cần thiết và tương xứng» không chuyển dịch một cách máy móc các tiêu chuẩn châu Âu; và cuối cùng, một sự bảo vệ dựa trên một Sắc lệnh hành pháp có thể bị thu hồi bởi Sắc lệnh hành pháp tiếp theo. Một bản án của CJEU về Quyết định mới —vụ việc mà nhiều người đã gọi với sự cam chịu là Schrems III— dự kiến sẽ có trong vài năm tới. Kết quả không thể được dự đoán trước. Trong mọi trường hợp, cấu trúc của lập luận rất giống với vụ việc năm 2020.

## Những gì các SME châu Âu không nghe thấy

Trong khi đại hội đồng CJEU đang thảo luận, văn phòng luật quy mô trung bình vẫn tiếp tục trao đổi thư từ với khách hàng thông qua Microsoft 365 được đặt tại các khu vực châu Âu nhưng thuộc sở hữu của một công ty Hoa Kỳ chịu sự điều chỉnh của FISA 702. Phòng khám tư nhân đồng bộ lịch hẹn qua Google Workspace. Cố vấn thuế gửi các tờ khai đã ký thông qua DocuSign. Nhà tâm lý học lập hóa đơn từ một bảng tính trong Notion. Văn phòng luật lao động lưu trữ hồ sơ trong Dropbox. Và hầu như tất cả họ đều chăm sóc khách hàng qua WhatsApp. Tất cả những điều này có thể hoạt động dưới sự bảo hộ của Quyết định Tương xứng 2023/1795, theo các nhà

cung cấp. Ngày mà Quyết định đó sụp đổ trong vụ Schrems III, tất cả các mối quan hệ đó sẽ bị bỏ mặc mà không có sự bảo vệ nào ngay lập tức.

Vấn đề không phải là tu từ. Từ năm 2022 đến 2024, một số cơ quan có thẩm quyền châu Âu đã giải quyết các hồ sơ chống lại các bên kiểm soát dữ liệu vì sử dụng Google Analytics mà không có công cụ chuyển giao phù hợp, áp dụng đúng lập luận của CJEU ngay cả trước khi Privacy Framework có hiệu lực. Cơ quan của Pháp, CNIL, là đơn vị đầu tiên chính thức hóa tiêu chí này vào năm 2022; các cơ quan của Áo, Ý và các nước khác cũng nối gót ngay sau đó. Sự không tuân thủ, dưới thiết kế vận hành hiện tại của các SME châu Âu, được ghi nhận theo thời gian thực đối với bất kỳ ai biết cách quan sát.

## TIA như một công cụ, không phải một nghi thức

Một phần đáng kể các bản TIA đang lưu hành trong các văn phòng châu Âu, nếu đọc kỹ, chỉ là các bài tập mang tính hình thức. Chúng liệt kê các công cụ hợp đồng, liệt kê các chứng chỉ của nhà cung cấp, trích dẫn các đảm bảo kỹ thuật, đánh dấu vào các ô. Rất ít bên tự hỏi nghiêm túc xem liệu một lệnh FISA 702 có buộc nhà cung cấp phải giao nộp dữ liệu hay không. Càng ít bên tự hỏi điều gì sẽ xảy ra với việc chuyển giao đó dưới một cuộc rà soát giả định về Privacy Framework. Điều khoản 5 của GDPR yêu cầu bên kiểm soát dữ liệu phải có khả năng chứng minh sự tuân thủ. Một bản TIA không được thực hiện nghiêm túc thì không chứng minh được điều gì; những gì nó chứng minh là ý muốn tuân thủ trên giấy tờ trong khi thực hiện ngược lại trên thực tế.

Phiên bản chân thực của TIA bắt đầu bằng một câu hỏi đơn giản: điều gì sẽ xảy ra nếu ngày mai nhà cung cấp này nhận được lệnh FISA 702 đối với các dữ liệu cụ thể này? Nếu câu trả lời trung thực là «họ sẽ phải giao nộp mà không thông báo cho chúng ta», thì các điều khoản hợp đồng không giải quyết được vấn đề. Những gì thực sự giải quyết được vấn đề, trong những trường hợp mà câu hỏi đó thực sự quan trọng, là không đặt dữ liệu vào tay nhà cung cấp đó.

## Thay đổi chính trị như một rủi ro cấu trúc

Có một tầng bổ sung, mang tính chính trị, cần được gọi tên mà không gây kịch tính. Quyết định Tương xứng 2023/1795 cuối cùng dựa trên Sắc lệnh hành pháp 14086, được Tổng thống Biden ký vào tháng 10 năm 2022. Một Sắc lệnh hành pháp được ký bởi một tổng thống và có thể bị thu hồi, sửa đổi hoặc làm mất nội dung bởi tổng thống tiếp theo. Do đó, việc bảo vệ dữ liệu châu Âu tại Hoa Kỳ phụ thuộc vào một quyết định hành chính mà cả Quốc hội Mỹ không đảm bảo lẫn hệ thống pháp luật Mỹ không bảo vệ với sự vững chắc như cách nó bảo vệ các vấn đề nội bộ khác. Từ tháng 1 năm 2025, một chính quyền mới đang điều hành Hoa Kỳ, và câu hỏi về tính liên tục thực tế của EO 14086 đã không còn là giả thuyết mà trở thành vấn đề đương đại. Bất kỳ kịch bản nào mà chính quyền quyết định rút lại hoặc giảm bớt Sắc lệnh đều sẽ khiến Quyết định của châu Âu mất đi nền tảng mà nó được xây dựng trên đó.

Đây không phải là một lập luận mang tính âm mưu. Đó là cách đọc tỉnh táo về thiết kế pháp lý. Các khung bảo vệ dữ liệu xuyên Đại Tây Dương đã sụp đổ hai lần: Safe Harbor năm 2015 (bản án Schrems I), Privacy Shield năm 2020 (Schrems II). Cái thứ ba dựa trên một mảnh ghép mong manh hơn hai cái trước. Một công ty châu Âu đặt cược việc xử lý dữ liệu của mình vào mảnh ghép đó ngày nay đang đưa ra một quyết định quản lý rủi ro, chứ không đơn thuần là tuân thủ quy định.

## Dành cho độc giả chuyên nghiệp

Các câu hỏi vận hành cần đặt ra trước khi chọn một dịch vụ đám mây cho dữ liệu chuyên môn —với sự khắt khe mà một thanh tra bảo vệ dữ liệu sẽ đặt ra— như sau:

1. Dữ liệu được lưu trữ vật lý ở đâu? Một khu vực tại châu Âu không phải là câu trả lời thỏa đáng nếu đơn vị điều hành là của Hoa Kỳ.

2. Ai điều hành dịch vụ, được thành lập tại khu vực pháp lý nào và có thể phải tuân theo các lệnh pháp lý nào?
3. Công cụ chuyển giao nào được viện dẫn: Quyết định Tương xứng 2023/1795, SCC với TIA, hay ngoại lệ theo điều khoản 49 của GDPR? Lựa chọn đó có thể biện minh được trước một cuộc thanh tra không?
4. Nếu Quyết định Tương xứng bị hủy bỏ vào ngày mai, kế hoạch vận hành hiện có là gì để duy trì hoạt động?
5. Có giải pháp thay thế nào của châu Âu hoặc tự lưu trữ cho chức năng đó không, và chi phí thực tế để chuyển đổi là bao nhiêu?

Không phải mọi chức năng của văn phòng hằng ngày đều đòi hỏi cùng một câu trả lời. Một bảng tính cho kế toán nội bộ có lẽ không đẩy câu hỏi lên mức độ này. Hồ sơ hình sự của khách hàng, hồ sơ bệnh án, bảng lương nhân viên thì có. Tính tương xứng là hợp lệ; sự trì trệ tập thể khiến các SME châu Âu vẫn phụ thuộc vào các nhà cung cấp Hoa Kỳ cho mọi thứ —ngay cả những thứ nhạy cảm nhất— thì không.

---

*Schrems II sẽ tròn sáu tuổi vào tháng 7 tới. Bản án này không làm thay đổi thói quen hằng ngày của phần lớn các doanh nghiệp châu Âu. Tuy nhiên, nó đã thay đổi bản đồ rủi ro mà các doanh nghiệp này phải đối mặt. Khi một quyết định hành chính của Hoa Kỳ xen vào giữa quy định của châu Âu và hoạt động thực tế của một doanh nghiệp vừa và nhỏ (SME), ít nhất ta nên biết rằng quyết định đó tồn tại và nó rất mong manh. Những ai đã chọn một kiến trúc không có bên điều hành trung gian —sợi chỉ xuyên suốt Cuadernos Lacre— hẳn sẽ muốn không phải viết những loại phân tích này mỗi khi một Schrems nào đó đệ đơn kháng cáo. Nhưng chúng tôi sẽ vẫn tiếp tục thực hiện chúng.*

## Nguồn tham khảo và đọc thêm

- Tòa án Công lý Liên minh Châu Âu — bản án ngày 16 tháng 7 năm 2020, vụ việc C-311/18, *Data Protection Commissioner chống lại Facebook Ireland Ltd. và Maximillian Schrems*.
- Quy định (EU) 2016/679, Chương V, từ điều khoản 44 đến 50 — chuyển giao dữ liệu cá nhân quốc tế.
- Quyết định thực thi (EU) 2023/1795 của Ủy ban, ngày 10 tháng 7 năm 2023, về mức độ bảo vệ dữ liệu cá nhân phù hợp trong khung EU-US Data Privacy Framework.
- Ủy ban Bảo vệ Dữ liệu Châu Âu — *Khuyến nghị 01/2020 về các biện pháp bổ sung cho các công cụ chuyển giao nhằm đảm bảo tuân thủ mức độ bảo vệ dữ liệu cá nhân của EU*, được thông qua vào ngày 18 tháng 6 năm 2021.
- noyb.eu — đơn kiện đệ trình ngày 7 tháng 9 năm 2023 chống lại Quyết định (EU) 2023/1795 trước các cơ quan bảo vệ dữ liệu châu Âu.
- *Foreign Intelligence Surveillance Act*, mục 702 (được mã hóa tại 50 U.S.C. § 1881a), và Sắc lệnh hành pháp 12333 về các hoạt động tình báo của Hoa Kỳ bên ngoài lãnh thổ quốc gia.

← TrướcKhi không có ai ở giữaTiếp theo →Thực sự SHA-256 là gì

## Các bài đọc gần đây

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Tải bài viết này để sử dụng ở bất cứ đâu bạn cần.

↓ Markdown ↓ Văn bản thuần túy ↓ PDF

Tệp sẽ được tải xuống thiết bị của bạn. Từ đó, bạn có thể lưu trữ, nhập vào Solo2 hoặc chia sẻ ở bất cứ đâu. Cuadernos không quyết định điểm đến thay cho bạn.

Dấu sáp · SHA-256 02c2ecdf5a3d22e5b3184c88c63844ce4c59c55dd28692534070b1eea10e9a4f

Cuadernos Lacre · Một ấn phẩm của Menzuri Gestión S.L. ·
viết bởi R.Eugenio · được biên tập bởi đội ngũ Solo2.

Trang web này không sử dụng cookie và không tải tài nguyên từ bên thứ ba. Chúng tôi sử dụng bộ đếm lượt truy cập ẩn danh tự lưu trữ (Umami, trên máy chủ Châu Âu của chúng tôi) và lượng JavaScript tối thiểu cần thiết cho lựa chọn giao diện sáng/tối của bạn. Không trình theo dõi, không hồ sơ hóa, không chia sẻ dữ liệu. Nếu bạn muốn theo dõi chúng tôi: RSS.