

# Cấu trúc kép của chủ quyền số

Cuộc thoát khỏi Palantir của Châu Âu và xiềng xích Big Tech Mỹ

Luật sư Kim Kyung-jin · Luật sư

# Mục lục

## **Chương 1: Sự thoát khỏi Palantir của châu Âu và tự chủ an ninh**

- 1.1 Quyết định của Tổng cục An ninh Nội địa Pháp (DGSI): Chuyển sang ArgonOS của ChapsVision
- 1.2 Sự rút lui của Cơ quan Bảo vệ Hiến pháp Liên bang Đức (BfV) và sự loại bỏ khỏi Đám mây Quốc phòng Liên bang
- 1.3 Chiến lược thay thế hoàn toàn trong vòng 2 năm của Bộ Quốc phòng Hà Lan và tuyển phòng thủ từ chối triệt để của Thụy Sĩ

## **Chương 2 Từ giả định đến thực tế: Cú sốc từ các biện pháp trừng phạt bằng công tắc ngắt của Mỹ**

- 2.1 Vụ chặn 'Fable 5' của Anthropic và lời cảnh báo dành cho các đồng minh
- 2.2 Bẫy lập pháp ngoài lãnh thổ: Thực chất thẩm quyền tài phán của Đạo luật CLOUD và Điều 702 FISA của Mỹ
- 2.3 'Air-Gap' và kiến trúc độc lập: Sự cách ly kỹ thuật vượt trên các điều khoản hợp đồng

## **Chương 3 Cấu trúc kép của chủ quyền kỹ thuật số: Tự chủ quốc gia và vết rạn nứt trong liên minh NATO**

- 3.1 Sự khác biệt giữa lĩnh vực tình báo trong nước và lĩnh vực liên minh quân sự
- 3.2 NATO đạt khả năng vận hành hoàn toàn 'Hệ thống thông minh Maven (MSS)' và cái bẫy về tính tương tác
- 3.3 Điều khoản ngoại lệ về an ninh trong Đạo luật Trí tuệ Nhân tạo (AI Act) của Liên minh Châu Âu và điểm mù trong kiểm soát

## **Chương 4. Sự đáp trả của Châu Âu: Gói chủ quyền công nghệ và khung 4 giai đoạn của CADA**

- 4.1 Đạo luật Phát triển Điện toán đám mây và AI (CADA) cùng đổi mới quy định tại các khu vực tăng tốc trung tâm dữ liệu
- 4.2 Thiết kế 4 cấp độ bảo đảm chủ quyền (Sovereignty Assurance Levels) của CADA
- 4.3 'Quyền chấm dứt hợp đồng vì lý do chủ quyền (Sovereignty Termination Clause)' và việc thể chế hóa nghĩa vụ về tính khả di

## **Chương 5 EuroStack và thách thức xây dựng hệ sinh thái thay thế độc lập**

5.1 Ý tưởng 'EuroStack' của Francesca Bria và rào cản đầu tư 300 tỉ euro

5.2 Liên minh phần mềm thay thế: Arcadia và hàng hóa công nghệ thuật số mã nguồn mở

5.3 Chủ quyền kinh tế chống lại các tập đoàn đa quốc gia né thuế: Báo cáo CICTAR và việc bảo vệ tài chính công

### **Kết luận: Từ quản lý sự phụ thuộc đến tính mở có khả năng phục hồi**

Kết luận 1: Tuyên bố trước khi các giải pháp thay thế trưởng thành, vượt qua giai đoạn rủi ro 2-3 năm tới

Kết luận 2: Con đường tự chủ bền vững duy trì tính mở (Resilient Openness)

## 1.1 Quyết định của Tổng cục An ninh Nội địa Pháp (DGSI): Chuyển sang ArgonOS của ChapsVision

Tổng cục An ninh Nội địa Pháp (DGSI) là cơ quan được thành lập vào năm 2014 thông qua việc cải tổ tổ chức tiền thân phụ trách công tác tình báo nội địa. Nhiệm vụ của cơ quan này là giám sát các mối đe dọa khủng bố, đồng thời ứng phó với hoạt động tình báo nước ngoài và các cuộc tấn công mạng. Từ năm 2016, DGSI đã sử dụng Gotham, phần mềm phân tích dữ liệu của công ty Mỹ Palantir. Cơ duyên áp dụng phần mềm này xuất phát từ vụ tấn công khủng bố xảy ra tại Paris vào tháng 11 năm 2015. Khi đó, DGSI cần gấp một công cụ để theo dõi nhật ký thông tin liên lạc, lộ trình di chuyển và dòng tiền của các tổ chức khủng bố trên cùng một màn hình, và phần mềm của Palantir đã đáp ứng nhu cầu đó.

Chính phủ Pháp không hề buông thả sự phụ thuộc này ngay từ đầu. Năm 2021, Bộ Nội vụ đã mở thầu dự án OTDH nhằm tìm kiếm công nghệ của doanh nghiệp Pháp có khả năng xử lý lượng dữ liệu khổng lồ với nhiều định dạng khác nhau trong một hệ thống quốc gia duy nhất. Tham gia đợt đấu thầu này có ChapsVision, cùng với Athea (liên doanh do tập đoàn quốc phòng khổng lồ Thales và công ty công nghệ thông tin Eviden thành lập) và công ty phần mềm Blueway. Tuy nhiên, không có ứng viên nào phát triển đủ nhanh để tiếp quản toàn bộ công việc hằng ngày của DGSI.

Bối cảnh khiến DGSI một lần nữa bắt tay với Palantir vào tháng 12 năm 2025 xuất phát từ thực tế là công nghệ thay thế vẫn chưa thể cắm rễ hoàn toàn trong hoạt động thực địa.

Ngày 15 tháng 12 năm 2025, Palantir thông báo đã gia hạn hợp đồng nhiều năm với DGSI. Đó là hợp đồng có thời hạn 3 năm. Tuy nhiên, đến tháng 6 năm 2026, chưa đầy sáu tháng sau khi ký hợp đồng mới, Chính phủ Pháp đã đưa ra một quyết định đi ngược lại hoàn toàn với hợp đồng này.

Nguyên nhân khởi nguồn là biện pháp của Chính phủ Mỹ. Ngày 9 tháng 6 năm 2026, công ty trí tuệ nhân tạo Anthropic của Mỹ đã ra mắt các mô hình ưu việt nhất của mình là Fable 5 và Mythos 5. Thế nhưng ba ngày sau, vào lúc 5 giờ 12 phút chiều ngày 12 tháng 6 (giờ bờ Đông nước Mỹ), Chính phủ Mỹ đã đưa ra chỉ thị kiểm soát xuất khẩu với lý do an ninh quốc gia, yêu cầu ngừng ngay lập tức quyền truy cập Fable 5 và Mythos 5 đối với người có quốc tịch nước ngoài. Vì không có cách nào xác định nhanh quốc tịch của người dùng, Anthropic đã chọn

giải pháp tạm thời chặn toàn bộ quyền truy cập của người dùng nước ngoài, bao gồm cả châu Âu.

Các nhà nghiên cứu và cơ quan hành chính ở châu Âu đang muốn trải nghiệm mô hình mới vừa ra mắt đã rơi vào cảnh bị chặn quyền truy cập chỉ sau ba ngày. Sự gián đoạn truy cập này đã được khôi phục khi lệnh kiểm soát xuất khẩu được dỡ bỏ vào khoảng ngày 1 tháng 7, nhưng phía châu Âu đã tận mắt chứng kiến thực tế rằng một quốc gia đồng minh có thể cắt quyền truy cập vào công nghệ cốt lõi chỉ bằng một đạo luật.

Vài tháng trước khi sự việc này xảy ra, Nghị viện Châu Âu đã định hướng giảm bớt sự phụ thuộc vào công nghệ nước ngoài. Ngày 22 tháng 1 năm 2026, Nghị viện Châu Âu đã thông qua nghị quyết về chủ quyền công nghệ và hạ tầng kỹ thuật số của châu Âu với 471 phiếu thuận, 68 phiếu chống và 71 phiếu trắng. Nghị quyết này bày tỏ sự lo ngại trước tình trạng phụ thuộc quá mức vào một số ít doanh nghiệp nước ngoài trong các lĩnh vực hạ tầng điện toán đám mây, bán dẫn, trí tuệ nhân tạo và an ninh mạng, đồng thời đề xuất nguyên tắc ưu tiên phần mềm mã nguồn mở trong mua sắm công cùng quỹ công nghệ chủ quyền trị giá 10 tỷ euro.

Quyết định của Pháp là một ví dụ về việc thực thi ở cấp độ từng quốc gia, được đưa ra năm tháng sau khi nghị quyết này được thông qua.

Chính phủ Pháp đã theo dõi tình hình trong bốn ngày trước khi hành động. Ngày 16 tháng 6 năm 2026, Thủ tướng Sébastien Lecornu thông báo rằng công cụ của Palantir mà DGSI đang sử dụng sẽ được thay thế bằng ArgonOS của công ty Pháp ChapsVision. Thời điểm đưa ra thông báo là một ngày trước khi khai mạc VivaTech, triển lãm công nghệ lớn nhất châu Âu diễn ra tại Paris. Trước đó một ngày, vào ngày 15 tháng 6, ChapsVision đã có tên trong Next40, chỉ số các doanh nghiệp đổi mới sáng tạo của Pháp.

Next40 là danh sách hỗ trợ do Chính phủ Pháp vận hành từ năm 2019, chỉ những kỳ lân có định giá doanh nghiệp vượt quá 1 tỷ euro hoặc các công ty gọi được vốn đầu tư trên 100 triệu euro trong vòng 3 năm mới có thể góp mặt. Việc hai tin tức này diễn ra liên tiếp trong vòng hai ngày đã tạo ra ấn tượng rằng quyết định này là một kế hoạch được chính phủ chuẩn bị từ lâu. Thủ tướng Lecornu tuyên bố rằng không thể chấp nhận thêm một sự phụ thuộc chiến lược nào khác trong lĩnh vực công nghệ thông tin, đồng thời khẳng định thời đại dựa dẫm vào thiện chí của các nước đồng minh đã kết thúc.

Có một thực tế cần phải làm rõ ở đây: thông báo và việc chấm dứt hợp đồng không phải là cùng một sự việc. Ngày 17 tháng 6, một ngày sau thông báo, tờ Le

Monde đưa tin phía Palantir khẳng định hợp đồng gia hạn vào tháng 12 năm 2025 vẫn có hiệu lực về mặt pháp lý. Tuyên bố công khai của Chính phủ Pháp về nhà cung cấp mới và việc chấm dứt thực tế hợp đồng cũ đòi hỏi các thủ tục hoàn toàn khác nhau. Bộ Nội vụ Pháp cũng thừa nhận thời hạn còn lại của hợp đồng gia hạn với Palantir, đồng thời cho biết cần có các thủ tục hành chính riêng để thanh lý hợp đồng.

Quá trình thay thế thực tế sẽ mất nhiều thời gian hơn. Bộ Nội vụ Pháp dự báo việc triển khai phần mềm mới vào hoạt động thực địa và di chuyển dữ liệu hiện có sẽ mất từ 18 đến 24 tháng. Các báo cáo khác lại cho rằng xét trên toàn bộ cấu trúc hợp đồng, quá trình chuyển đổi hoàn toàn sẽ kéo dài từ năm 2027 đến năm 2029. Bộ trưởng Nội vụ Laurent Nuñez cam kết sẽ có một giai đoạn quá độ vận hành song song cả hai hệ thống cho đến năm 2027. Lý do quá trình chuyển giao kéo dài là vì đây không chỉ đơn thuần là việc thay thế một phần mềm.

DGSI phải thực hiện lần lượt năm bước: chuyển đổi phương thức thao tác cũ sang giao diện mới, đào tạo lại đội ngũ nhân viên, thiết lập luồng truy xuất dữ liệu mới, đảm bảo các cuộc điều tra đang diễn ra không bị gián đoạn, và kiểm tra khả năng chịu tải công việc thực tế. Các nhân viên của DGSI đã quen với giao diện và cách vận hành của Palantir, trong khi bản thân phương thức lưu trữ thông tin cũng được thiết kế theo tiêu chuẩn của hệ thống Mỹ. Nếu vội vã cắt đứt liên kết, nguy cơ tạo ra khoảng trống trong hoạt động tình báo là rất lớn, do đó Chính phủ Pháp đã chọn phương án chuyển đổi theo từng giai đoạn.

Nền tảng mới mà ChapsVision đang phát triển dự kiến sẽ tích hợp tính năng agent AI thực hiện một phần công việc tìm kiếm và phân tích, và quy trình xác minh xem tính năng này có hoạt động ổn định trong các cuộc điều tra thực tế như công cụ của Palantir hay không cũng là một yếu tố khiến thời gian chuyển giao bị kéo dài.

Yếu tố hậu thuẫn cho quyết định này là kế hoạch đầu tư France 2030. Chính phủ đã phân bổ thêm 655 triệu euro để đạt được sự tự chủ trong lĩnh vực trí tuệ nhân tạo. Một phần trong số vốn này được sử dụng để phát triển công cụ AI tương tác dành cho công chức. Ngày 16 tháng 6 năm 2026, Bộ trưởng phụ trách Công vụ David Amiel thông báo sẽ mở rộng chatbot 'L'Assistant'—vốn được vận hành thử nghiệm trên quy mô 10.000 người—cho toàn bộ 1 triệu công chức. Chi phí cho giai đoạn mở rộng đầu tiên ước tính khoảng 700.000 đến 750.000 euro, và việc phát triển do công ty AI của Pháp Mistral AI đảm nhận.

Arthur Mensch, Tổng Giám đốc của Mistral AI, đã từng khẳng định rằng châu Âu phải thoát khỏi cơ cấu thuê hạ tầng điện toán đám mây của Mỹ để tự sở hữu hạ

tăng của riêng mình. Phát biểu này đã trở thành điểm tựa lý luận cho quyết định của DGSI.

ChapsVision, nhà cung cấp mới của Pháp, là công ty do Tổng giám đốc Olivier Dellenbach thành lập vào năm 2019. Ông Dellenbach từng có kinh nghiệm bán công ty phần mềm phân tích tài chính eFront cho BlackRock với giá 1,3 tỷ USD vào năm 2019. ChapsVision đã chọn chiến lược mở rộng quy mô thông qua thu mua thay vì tự phát triển. Sau khi lần lượt mua lại công ty phần mềm quản lý quan hệ khách hàng Coheris, công ty dữ liệu bán lẻ Octipas, công ty thương mại điện tử Sparkow và công ty tự động hóa tiếp thị NP6, ChapsVision tiếp tục thu mua Bertin IT và Vecsys, những doanh nghiệp sở hữu công nghệ an ninh mạng, tình báo và nhận dạng giọng nói.

Việc thu mua Bertin IT và Vecsys đã giúp doanh thu tăng từ 30 triệu euro lên 40 triệu euro, còn số lượng nhân viên tăng từ 260 người lên 380 người. Sau khi thực hiện hơn 25 thương vụ thu mua như vậy, công ty đã nhận được vốn đầu tư từ ngân hàng đầu tư nhà nước Pháp Bpifrance và Tikehau Capital, huy động thêm 100 triệu euro vào năm 2022, và doanh thu riêng trong năm 2025 đã đạt 200 triệu euro.

ArgonOS do ChapsVision phát triển là phần mềm thu thập và phân tích các thông tin có định dạng khác nhau. Nó xử lý tập trung không chỉ tài liệu mà cả hình ảnh, âm thanh và tình báo nguồn mở (OSINT - thông tin công khai trên Internet). Chương trình này hoạt động trong môi trường biệt lập (air-gap) ngắt kết nối với mạng bên ngoài, hoặc trên nền tảng đám mây chủ quyền do nhà nước trực tiếp quản lý. Toàn bộ cổ phần của công ty do các cổ đông châu Âu nắm giữ. Cơ cấu sở hữu này có ý nghĩa quan trọng chính vì Đạo luật CLOUD (CLOUD Act) của Mỹ. Đạo luật này quy định rằng nếu là dịch vụ do pháp nhân Mỹ vận hành, doanh nghiệp phải cung cấp thông tin theo yêu cầu của cơ quan điều tra Mỹ bất kể máy chủ đặt ở quốc gia nào.

Vì ArgonOS không phải là pháp nhân Mỹ, hệ thống này nằm ngoài phạm vi áp dụng của đạo luật nói trên.

Quy trình Tổng cục An ninh Nội địa Pháp (DGSI) lựa chọn ChapsVision cũng là điều cần xem xét. Công ty này đã trải qua quá trình đấu thầu dự án tích hợp thông tin OTDH do Bộ Nội vụ Pháp khởi xướng vào năm 2021. OTDH là dự án nhằm xử lý khối lượng dữ liệu khổng lồ với nhiều định dạng khác nhau trong một hệ thống quốc gia thống nhất, với tổng ngân sách được ấn định khoảng 40 triệu euro. Sau hơn 3 năm thẩm định, vào cuối năm 2024, ChapsVision đã giành được hợp đồng

Gói 1 (Lot 1) về xử lý và sắp xếp dữ liệu gốc. Cuộc cạnh tranh quanh Gói 2 (Lot 2) còn diễn ra gay gắt hơn.

Vào giai đoạn cuối của gói thầu này, chỉ còn lại ba ứng viên: Athea (liên doanh giữa Thales và Eviden), công ty phần mềm Blueway và ChapsVision. Đến tháng 6 năm 2026, ChapsVision tiếp tục chiến thắng trong cuộc đua này để giành quyền thực hiện Gói 2 (Lot 2) về trực quan hóa và mô hình hóa thông tin, trở thành đơn vị trúng thầu cuối cùng. Nhờ kết quả trúng thầu này, ArgonOS đã vượt ra ngoài phạm vi của Tổng cục An ninh Nội địa để trở thành hệ thống nền tảng đảm nhận việc xử lý dữ liệu cho nhiều cơ quan tư pháp khác nhau.

Quyết định này của Pháp cũng đã ảnh hưởng sang các nước láng giềng. Vào tháng 5 năm 2026, Cơ quan Bảo vệ Hiến pháp Liên bang Đức đã chốt kế hoạch triển khai cùng hệ thống ArgonOS, thậm chí sớm hơn cả Pháp. Bối cảnh và quá trình diễn ra quyết định này sẽ được đề cập trong phần tiếp theo.

Việc loại bỏ hoàn toàn công nghệ Mỹ khỏi bộ máy nhà nước Pháp không phải là điều có thể hoàn tất trong vài tháng. Thói quen vận hành đã quen thuộc của các đặc vụ, các tiêu chuẩn dữ liệu và thời hạn còn lại của các hợp đồng cũ đều là những rào cản còn tồn tại. Dù vậy, bản thân thực tế chính phủ Pháp đã công khai chuyển hướng là điều không thể đảo ngược. Việc khi nào hợp đồng với Palantir mới chấm dứt hoàn toàn và quá trình chuyển giao thực tế sang ArgonOS diễn ra suôn sẻ đến đâu vẫn là những thực tế cần tiếp tục theo dõi và xác minh trong thời gian tới.

---

## **Căn cứ và tài liệu tham khảo**

1. Jon Henley, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026-06-16, <https://www.theguardian.com/world/2026/jun/16/france-ai-data-tools-palantir-chapsvision>
2. Palantir Technologies, 'Palantir Announces Renewal of Multi-Year Contract with the DGSI', Business Wire, 2025-12-15, <https://www.businesswire.com/news/home/20251215083215/en>
3. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, <https://www.anthropic.com/news/fable-mythos-access>
4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, <https://www.anthropic.com/news/redeploying-fable-5>
5. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, [https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice\\_6754592\\_7.html](https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html)
6. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, 2026-06-16, <https://www.chapsvision.com/press-release/chapsvision-chosen-by-france-to-deploy-argonos-for-otdh-project/>
7. Tác giả khuyết danh, 'L'Etat français déploie Mistral AI auprès d'un million de fonctionnaires', ChannelNews, 2026-06-16, [https://www.channelnews.fr/letat-francais-deploie-mistral-ai-aupres-dun-](https://www.channelnews.fr/letat-francais-deploie-mistral-ai-aupres-dun)

million-de-fonctionnaires-et-inclut-la-souverainete-numerique-dans-les-objectifs-2026-2029-de-lugap-157317

8. BlackRock, 'BlackRock to Acquire eFront -- Industry Leading Alternatives Investment Software Provider', Business Wire, 2019-03-22, <https://www.businesswire.com/news/home/20190322005228/en/BlackRock-to-Acquire-eFront---Industry-Leading-Alternatives-Investment-Software-Provider>
9. Tác giả khuyết danh, 'DGSi : Palantir éjecté, ChapsVision prend le relais en 2029', info.fr, 2026, <https://info.fr/palantir-ejecte-dgsi-france-rompt-dependance-americaine-chapsvision/>
10. Tác giả khuyết danh, 'French Security Service to Replace Palantir With Local Software', Bloomberg, 2026-06-16, <https://www.bloomberg.com/news/articles/2026-06-16/french-security-service-to-replace-palantir-with-local-software>
11. Tác giả khuyết danh, 'ChapsVision to replace Palantir in major contract with French intelligence agency', Sifted, 2026, <https://sifted.eu/articles/chapsvision-to-replace-palantir-in-major-contract-with-french-intelligence-agency>
12. Tác giả khuyết danh, 'Quatre choses à savoir sur Palantir, ce géant technologique américain controversé qui travaille avec la DGSi', franceinfo, 2026, [https://www.franceinfo.fr/societe/armee-securite-defense/quatre-choses-a-savoir-sur-palantir-ce-geant-technologique-americain-controverse-qui-travaille-avec-la-dgsi\\_7682872.html](https://www.franceinfo.fr/societe/armee-securite-defense/quatre-choses-a-savoir-sur-palantir-ce-geant-technologique-americain-controverse-qui-travaille-avec-la-dgsi_7682872.html)
13. ChapsVision, 'ChapsVision acquiert Bertin IT et Vecsys', ChapsVision, 2021, <https://www.chapsvision.fr/acquisition-bertin-it-et-vecsyst-par-chapsvision/>
14. La mission French Tech, 'French Tech Next40/120', La mission French Tech, 2026, <https://lafrenchtech.gouv.fr/en/programme/french-tech-next40-120/>
15. Tác giả khuyết danh, 'Anthropic releases Claude Fable, a version of Mythos, days after warning AI is becoming too dangerous', TechCrunch, 2026-06-09, <https://techcrunch.com/2026/06/09/anthropics-claude-fable-5-is-a-version-of-mythos-the-public-can-access-today/>
16. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', European Parliament, 2026-01-22, [https://www.europarl.europa.eu/doceo/document/TA-10-2026-0022\\_EN.html](https://www.europarl.europa.eu/doceo/document/TA-10-2026-0022_EN.html)
17. GIFAS, 'Athea, ChapsVision et Blueway retenus par la DGSi pour la seconde phase du programme OTDH', GIFAS, 2026, <https://gifas.fr/press-summary/athea-chapsvision-et-blueway-retenus-par-la-dgsi-pour-la-seconde-phase-du-programme-otdh>
18. Tác giả không xác định, 'La France tourne la page Palantir : ChapsVision remporte le marché de la DGSi pour sa plateforme de traitement et d'exploitation de données', Usine Digitale, 2026, <https://www.usine-digitale.fr/souverainete/la-france-tourne-la-page-palantir-chapsvision-remporte-le-marche-de-la-dgsi-pour-sa-plateforme-de-traitement-et-dexploitation-de-donnees.I3EESPQQIBEX3AQXHIF6ABGI3M.html>

## 1.2 Sự rút lui của Cơ quan Bảo vệ Hiến pháp Liên bang Đức (BfV) và sự loại bỏ khỏi Đám mây Quốc phòng Liên bang

Tại Đức, cơ quan tình báo nội địa và quân đội đã giữ khoảng cách với Palantir ở những thời điểm khác nhau, nhưng theo cùng một hướng. Hai quyết định này không phải là một sự kiện duy nhất mà là hai sự thật riêng biệt trải qua các quy trình khác nhau.

Cơ quan Bảo vệ Hiến pháp Liên bang Đức (BfV) là cơ quan cấp cao nhất đảm nhận thông tin tình báo nội địa. Đảm nhận việc giám sát chuyển động của các lực lượng cực đoan và ngăn chặn hoạt động gián điệp nước ngoài, cơ quan này có vị trí tương tự Tổng cục An ninh Nội địa của Pháp. Cục trưởng Sinan Selen vào tháng 12 năm 2025, tại một cuộc họp nội bộ của Đức, đã phát biểu rằng các cơ quan an ninh phải định hình rõ ràng hơn quan điểm của châu Âu và thoát khỏi sự phụ thuộc lâu dài. Năm tháng sau phát biểu này, vào tháng 5 năm 2026, Cơ quan Bảo vệ Hiến pháp Liên bang đã quyết định thu mua ArgonOS của công ty Pháp ChapsVision thay vì chương trình của Palantir. Điều này được ghi nhận là trường hợp đầu tiên một cơ quan liên bang của Đức chính thức từ chối Palantir.

ArgonOS mà Cơ quan Bảo vệ Hiến pháp Liên bang lựa chọn là chương trình giống như đã được giải thích ở phần trước. Nó tích hợp và phân tích thông tin có định dạng khác nhau, đồng thời sở hữu cả tính năng tình báo nguồn mở nhằm theo vết thông tin công khai trên Internet. Điểm đáng chú ý ở phía Đức là sự hợp tác được thiết lập trong quá trình triển khai thực tế chương trình này. ChapsVision đã bắt tay với Rola Security Solutions, công ty công nghệ thông tin đã quản lý cơ sở dữ liệu cảnh sát Đức PIAV trong một thời gian dài. Bằng cách hợp tác với một công ty đã định hình vững chắc trong mạng lưới an ninh của Đức, họ đã giúp chương trình mới vận hành mượt mà trên nền tảng hệ thống hiện có.

Việc thu mua này không dẫn đến việc triển khai ngay lập tức trên thực địa. Chính phủ Liên bang Đức đang chuẩn bị một dự luật sửa đổi dài hơn 700 trang nhằm tái xác định thẩm quyền của Cơ quan Tình báo Liên bang (BND) và Cơ quan Bảo vệ Hiến pháp Liên bang. Dự luật này trao cho hai cơ quan quyền can thiệp trực tiếp trong các tình huống đe dọa cùng các công cụ mới để xử lý trí tuệ nhân tạo và thông tin sinh trắc học, đồng thời quy định bắt buộc chia sẻ thông tin giữa Cơ quan Bảo vệ Hiến pháp Liên bang, các cơ quan tình báo bang và Cơ quan Phản gián Quân sự (MAD). Do Tòa án Hiến pháp Liên bang Đức đã ấn định thời hạn sửa

đổi luật này là cuối năm 2026, Quốc hội Liên bang sẽ xử lý dự luật này ngay sau khi kỳ nghỉ hè kết thúc.

Các công cụ phân tích mới, bao gồm cả ArgonOS, chỉ có thể đi vào hoạt động hoàn toàn khi khung pháp lý này được thiết lập. Khi luật chưa được ban hành, giai đoạn quá độ phải trải qua bằng việc duy trì hệ thống cũ. Việc xác định thu mua và thời điểm việc thu mua đó thực sự đi vào vận hành được gắn liền với các quy trình riêng biệt như vậy.

Tách biệt với quyết định của Cơ quan Bảo vệ Hiến pháp Liên bang, Quân đội Liên bang Đức đã thực hiện các bước riêng để loại bỏ Palantir khỏi lĩnh vực quân sự. Năm 2017, Quân đội Liên bang Đức đã thành lập một quân chủng riêng gọi là Bộ Tư lệnh Không gian Mạng và Thông tin để chuyên trách phòng thủ mạng và vận hành hệ thống thông tin. Trong cuộc phỏng vấn với tờ báo kinh tế Đức Handelsblatt vào ngày 28 tháng 4 năm 2026, Phó Đô đốc Thomas Daum thuộc Bộ tư lệnh này tuyên bố rằng hiện tại hoàn toàn không có kế hoạch sử dụng Palantir cho dự án đám mây quân sự. Ông cho biết việc cấp quyền truy cập dữ liệu quốc gia của Đức cho nhân viên của một công ty tư nhân nước ngoài là điều không thể tưởng tượng được.

Phát biểu này đã loại Palantir khỏi danh sách ứng viên cho pCloudBw, dự án đám mây quốc phòng thế hệ tiếp theo do Quân đội Liên bang xúc tiến. pCloudBw là dự án nhằm tập hợp dữ liệu tác chiến phân tán khắp các đơn vị và năng lực xử lý trí tuệ nhân tạo lên một đám mây bảo mật duy nhất, và Palantir từng là một trong những ứng viên được xem xét cho đến trước khi bị loại.

Đằng sau sự loại bỏ này là những lo ngại liên quan đến Tổ chức Hiệp ước Bắc Đại Tây Dương (NATO). Vào tháng 3 năm 2025, NATO đã ký một hợp đồng ngắn hạn với Palantir và đưa Hệ thống Thông minh Maven vào hệ thống chỉ huy. Maven là chương trình xử lý thông tin hình ảnh vệ tinh và đề xuất thứ tự ưu tiên mục tiêu tấn công. Tuy nhiên, việc vận hành và quản lý hàng ngày của chương trình này do nhân sự kỹ thuật tư nhân thuộc Palantir đảm nhận chứ không phải quân nhân. Nhà chức trách quốc phòng Đức nhận định rằng cấu trúc giao quyền quản lý thông tin tác chiến cho một doanh nghiệp tư nhân của đồng minh có thể xâm hại đến chủ quyền phòng thủ của quốc gia. Cùng với đó, Đạo luật CLOUD (CLOUD Act) của Mỹ cũng trở thành một trở ngại.

Đạo luật này mở đường cho các cơ quan điều tra của Mỹ truy cập thông tin do pháp nhân Mỹ xử lý, bất kể vị trí của máy chủ. Bộ Quốc phòng nhận thấy tình huống mà các kế hoạch tác chiến của Quân đội Liên bang Đức nằm trong tầm ảnh hưởng của đạo luật này là điều khó có thể chấp nhận.

Sau khi loại bỏ Palantir, Quân đội Liên bang đã tìm kiếm các ứng viên thay thế ngay tại châu Âu. Vào khoảng ngày 29 tháng 4 năm 2026, khi phát biểu của Phó Đô đốc Daum được công bố, Quân đội Liên bang đã xem xét rộng rãi các giải pháp bao gồm hệ thống đám mây và trí tuệ nhân tạo Altra của công ty Đức Helsing, hệ thống đám mây chủ quyền S3NS của công ty Đức SAP, và BullSequana XH3000 của công ty Pháp Atos. Altra đã được triển khai tại một số đơn vị của Quân đội Liên bang, trong khi S3NS là hệ thống được tập đoàn quốc phòng Thales sử dụng để chuyển giao các nghiệp vụ tài chính và thu mua. Sau khi rà soát rộng rãi như vậy, danh sách ứng viên chung kết cho dự án pCloudBw đã được rút gọn xuống còn ba cái tên.

Almato, có trụ sở tại Stuttgart, là công ty con của tập đoàn Đức DATAGROUP, sở hữu chứng nhận xử lý dữ liệu cấp độ bảo mật VS-NfD theo yêu cầu của Cục An ninh Thông tin Liên bang Đức (BSI). Công ty khởi nghiệp Orcrist Technologies tại Berlin đã giới thiệu công nghệ kết hợp thông tin quy mô lớn với nhiều định dạng khác nhau vào một màn hình nhận thức tình huống duy nhất. ChapsVision ở Paris cũng tham gia cuộc cạnh tranh này với chương trình chủ lực ArgonOS. Ba công ty đã trải qua các đợt thử nghiệm liên kết dữ liệu thực tế trong mùa hè năm 2026, và đơn vị trúng thầu cuối cùng dự kiến sẽ được công bố vào cuối năm 2026.

Việc loại bỏ Palantir và việc chọn ai thay thế vẫn là hai vấn đề riêng biệt như vậy.

Giám đốc điều hành Alex Karp của Palantir đã phản ứng ngay lập tức trước quyết định này. Trong cuộc phỏng vấn với cơ quan truyền thông Đức Bild, ông nói rằng mình bất ngờ trước tin tức này và so sánh cuộc tranh luận ở Đức với câu chuyện về phép thuật. Giám đốc Karp khẳng định công nghệ của Palantir đã được kiểm chứng trên chiến trường Ukraine, đồng thời nhắc đến mối duyên nợ mà ông và nhà đồng sáng lập Peter Thiel đã duy trì với Đức. Phản bác lại điều này, Bộ trưởng Bộ Kỹ thuật số Đức Karsten Wildberger nhấn mạnh rằng sự tự chủ không bị đặt dưới sự kiểm soát đơn phương của doanh nghiệp nước ngoài là điều kiện tiên quyết hàng đầu phải bảo vệ trong an ninh quốc gia.

Phán quyết của cơ quan tư pháp cũng đóng một vai trò khiến Đức trở nên thận trọng hơn với Palantir. Bang Hessen đã mua hệ thống Gotham của Palantir vào năm 2017 và vận hành nó dưới tên gọi hessenDATA. Vào ngày 16 tháng 2 năm 2023, Tòa án Hiến pháp Liên bang Đức đã phán quyết vi hiến đối với các điều khoản luật mà bang Hessen và bang Hamburg sử dụng hệ thống này làm căn cứ cho hoạt động cảnh sát dự báo. Tòa án nhận định rằng phương thức phân tích diện rộng bản ghi thông tin liên lạc và dữ liệu cá nhân của công dân mà không có cơ sở pháp lý đã xâm phạm quyền tự quyết thông tin. Phán quyết này sau đó đã

trở thành khởi điểm để các bang của Đức rà soát lại các hệ thống dựa trên nền tảng Palantir.

Tuy nhiên, không phải tất cả các bang đều đi theo cùng một hướng. Ngày 20 tháng 3 năm 2025, Bộ Nội vụ bang Baden-Württemberg đã ký hợp đồng triển khai chương trình Gotham của Palantir mà không qua thảo luận trước với Đảng Xanh. Hợp đồng này không bao gồm điều khoản chấm dứt giữa chừng, với điều kiện thanh toán tổng cộng 25 triệu euro trong 5 năm, tương đương khoảng 9,25 triệu euro mỗi năm. Trong nội bộ Đảng Xanh, bên tham gia chính phủ liên minh bang, 92% đã bỏ phiếu ủng hộ ý kiến cho rằng phải dừng hợp đồng này ngay lập tức. Tuy nhiên, một hợp đồng thiếu điều khoản rút lui đã không thể bị hủy bỏ chỉ bằng sự phản đối về mặt chính trị, và chính quyền bang vẫn tiếp tục duy trì hợp đồng.

Trường hợp này cho thấy thực tế rằng nếu không đưa trước các điều kiện chấm dứt vào hợp đồng mua sắm công, nhà nước sẽ tự làm mất đi sức mạnh đàm phán của mình.

Có một điểm cần lưu ý ở đây. Đạo luật Trí tuệ Nhân tạo (AI Act) của Liên minh Châu Âu loại trừ các hệ thống trí tuệ nhân tạo được sử dụng cho mục đích quân sự, quốc phòng và an ninh quốc gia khỏi phạm vi áp dụng quy định. Điều 2 và khoản 24 phần mở đầu của đạo luật này tìm thấy căn cứ đó ở trách nhiệm an ninh quốc gia mà mỗi quốc gia thành viên tự gánh vác cùng với tính chất của các hoạt động quân sự. Nói cách khác, quyết định loại bỏ Palantir của Cơ quan Bảo vệ Hiến pháp Liên bang và Quân đội Liên bang không phải là kết quả tuân theo các quy định về trí tuệ nhân tạo ở cấp độ Liên minh Châu Âu, mà là lựa chọn do chính quốc gia Đức tự đưa ra trong lĩnh vực mua sắm và chính trị.

Động thái trái ngược này giữa các cơ quan liên bang và chính quyền bang cho thấy thực tế rằng ngay trong cùng một quốc gia, tốc độ và phương thức bảo vệ chủ quyền cũng có sự khác biệt. Cơ quan Bảo vệ Hiến pháp Liên bang và Quân đội Liên bang đã loại bỏ Palantir ở giai đoạn trước khi ký hợp đồng, nhưng bang Baden-Württemberg lại bị ràng buộc bởi hợp đồng đã ký kết.

---

## **Căn cứ và tài liệu tham khảo**

1. Tác giả không rõ, 'Digital Sovereignty: BfV Buys European Palantir Alternative', heise online, 2026, <https://www.heise.de/en/news/Digital-Sovereignty-BfV-Buys-European-Palantir-Alternative-11293717.html>
2. Markus Seyfferth, 'Wählt der BfV ArgonOS statt Palantir? Erstmals ja.', Dr. Web, 2026-05-01, <https://www.drweb.de/waehlt-der-bfv-argonos-statt-palantir-erstmals-ja/>
3. Tác giả không rõ, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, <https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die->

bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

4. Jonas Brandstetter, 'Bundeswehr verzichtet auf Palantir', Behörden Spiegel, 2026-05-12, <https://www.behoerden-spiegel.de/2026/05/12/bundeswehr-verzichtet-auf-palantir/>
5. Tác giả không rõ, 'Palantir CEO Alex Karp Critiques German Military's Rejection of Advanced Defense Technologies', SSBCrack News, 2026, <https://news.ssbcrack.com/palantir-ceo-alex-karp-critiques-german-militarys-rejection-of-advanced-defense-technologies/>
6. Bundesverfassungsgericht, 'Urteil vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20', Bundesverfassungsgericht, 2023-02-16, [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216\\_1bvr154719.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html)
7. Tác giả không rõ, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, <https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518>
8. Tác giả không rõ, 'Neue Regeln für BND und Verfassungsschutz: Regierung will Geheimdienst-Befugnisse massiv ausweiten', Tagesspiegel, 2026, <https://www.tagesspiegel.de/politik/neue-regeln-fur-bnd-und-verfassungsschutz-regierung-will-geheimdienst-befugnisse-massiv-ausweiten-15786692.html>
9. Tác giả không rõ, 'Geheimdienstreform: Zeitenwende für Spione', netzpolitik.org, 2026, <https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/>
10. Tác giả không rõ, 'Bundeswehr Will Not Use Palantir for Military Cloud and AI Project; European Alternatives Examined', Grosswald, 2026-04-29, <https://www.grosswald.org/bundeswehr-rejects-palantir-military-cloud-ai-project-european-alternatives/>
11. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

### **1.3 Chiến lược thay thế hoàn toàn trong vòng 2 năm của Bộ Quốc phòng Hà Lan và tuyến phòng thủ từ chối triệt để của Thụy Sĩ**

Hà Lan và Thụy Sĩ đã giữ khoảng cách với Palantir theo những cách khác với Pháp và Đức. Hà Lan đang lên kế hoạch loại bỏ chương trình vốn đang sử dụng, trong khi Thụy Sĩ trong nhiều năm qua đã liên tục lựa chọn không đưa Palantir vào ngay từ đầu.

Các cuộc thảo luận xung quanh Bộ Quốc phòng Hà Lan đã bùng lên khi cơ quan truyền thông điều tra Follow the Money tiết lộ rằng Bộ Tư lệnh Tác chiến Đặc biệt (SOCOM) thuộc Bộ Quốc phòng cũng đang sử dụng Palantir, và phía Palantir có thể tiếp cận thông tin nhạy cảm trong khi các chiến dịch quân sự diễn ra. Follow the Money trước đó cũng đã làm rõ việc quân đội và cảnh sát Hà Lan bí mật giao dịch với Palantir trong nhiều năm. Phía Bộ Quốc phòng giải thích rằng việc tiếp cận của nhân viên Palantir chỉ giới hạn trong những trường hợp ngoại lệ, họ không làm việc một mình mà dưới sự giám sát, và chỉ xử lý dữ liệu giả định hoặc dữ liệu cũ chứ không phải thông tin mật thực tế.

Tuy nhiên, những chỉ trích cho rằng việc nhân viên của một doanh nghiệp nước ngoài tiếp cận thông tin bí mật dưới bất kỳ hình thức nào cũng là mối đe dọa trực tiếp đối với an ninh quốc gia vẫn không lắng xuống. Thứ trưởng Bộ Quốc phòng Derk Boswijk cho biết ông đã đưa ra chỉ thị nội bộ nhằm giảm bớt việc sử dụng Palantir vào tháng 5 năm 2026, tức một tháng trước khi báo cáo này xuất hiện. Ông thừa nhận sự lo ngại về việc phụ thuộc vào Palantir và cho biết đã chỉ đạo tìm kiếm các giải pháp thay thế từ Châu Âu. Một lý do khác khiến vấn đề này gây tranh cãi là việc Palantir cung cấp cả tính năng sử dụng trí tuệ nhân tạo để lựa chọn mục tiêu tấn công.

Thứ trưởng Boswijk vào ngày 2 tháng 6 năm 2026 đã chính thức tuyên bố tại Hạ viện (Tweede Kamer) rằng ông sẽ thay thế Palantir bằng các giải pháp của Châu Âu càng sớm càng tốt. Dù đặt mục tiêu 2 năm để tìm kiếm giải pháp thay thế đạt mức độ tương đương hoàn toàn, ông cũng thừa nhận rằng trong lĩnh vực trí tuệ nhân tạo dùng cho quân sự, hiện chưa có giải pháp thay thế nào của Châu Âu đạt đến trình độ này. Ông cũng vạch rõ ranh giới với việc chấm dứt quan hệ ngay lập tức khi cho biết nếu cắt đứt mối quan hệ ngay lúc này, có thể xuất hiện khoảng trống an ninh, dù ở mức độ hạn chế, trong hệ thống tác chiến trận mạc, hậu cần quốc phòng và xử lý thông tin.

Nhìn vào tiến độ thực tế sau tuyên bố, có những đánh giá cho rằng tốc độ vẫn còn chậm chạp. Trong câu trả lời bổ sung mà chính phủ gửi tới Hạ viện, thay vì đưa ra thời hạn kết thúc cụ thể, chỉ có các cụm từ như "xem xét phương án thay thế" và "giảm sự phụ thuộc". Có một vài lý do khiến tiến độ bị chậm lại. Các hợp đồng ký kết với Palantir trong Bộ Quốc phòng được thực hiện riêng lẻ theo từng bộ phận, nên ngay cả danh sách hợp đồng thống nhất ở cấp chính phủ cũng không có. Điều này đồng nghĩa với việc không có cách nào để tập hợp và nhìn tổng thể các hợp đồng đang tiến hành, dự kiến hay đã kết thúc. Thêm vào đó, yêu cầu về khả năng tương tác - đòi hỏi các đơn vị quân đội phải sử dụng cùng một hệ thống để trao đổi thông tin với các đồng minh NATO - cũng đóng vai trò là một rào cản.

Lực lượng Hiến binh Hoàng gia (Marechaussee) chịu trách nhiệm quản lý biên giới cũng đang sử dụng các công cụ của Palantir trong hệ thống giám sát biên giới, khiến đây trở thành vấn đề không thể giải quyết chỉ bằng quyết định của riêng Bộ Quốc phòng. Đánh giá chung của các phương tiện truyền thông theo dõi vấn đề này là mặc dù về mặt chính trị hướng đi đã được xác định, nhưng động lực cụ thể để đưa nó vào thực thi vẫn còn yếu.

Thụy Sĩ là một trường hợp mang sắc thái khác. Thay vì loại bỏ các chương trình đã đưa vào sử dụng như Pháp hay Đức, trường hợp này giống với việc nhiều cơ quan chính phủ qua nhiều năm đã liên tục đưa ra quyết định không chấp nhận Palantir.

Cục Y tế Công cộng Liên bang Thụy Sĩ từ tháng 4 đến tháng 5 năm 2020 đã loại Palantir khỏi gói thầu quản lý hậu cần vắc-xin COVID-19. Mặc dù lý do cụ thể không được công bố, nhưng có thông tin cho rằng bộ phận phụ trách đã coi chính sự tham gia của Palantir là một vấn đề. Cùng năm đó, Cục Thống kê Liên bang Thụy Sĩ đã không đáp lại yêu cầu cuộc gặp từ phía Palantir. Cục Công nghệ Thông tin Liên bang Thụy Sĩ sau khi tiến hành ba cuộc họp với Palantir từ năm 2020 đến năm 2021 đã đưa ra kết luận rằng không cần thiết phải áp dụng. Armasuisse, Cơ quan Mua sắm Quốc phòng Thụy Sĩ, vào năm 2020 đã loại Palantir tham gia đấu thầu hệ thống công nghệ thông tin cho Cục Tình báo Quân đội.

Lý do loại bỏ là do không đáp ứng được các yêu cầu bắt buộc, và những yêu cầu đó là gì thì không được công khai.

Vào tháng 10 năm 2022, Văn phòng Báo cáo Phòng chống Rửa tiền Thụy Sĩ (MROS) đã nhận buổi trình diễn phần mềm của Palantir, nhưng đã không áp dụng vì nhận thấy thiếu cơ sở pháp lý để đưa vào sử dụng và có khả năng vi phạm pháp luật. Xu hướng này tiếp tục kéo dài đến năm 2024. Louis Mosley, người phụ trách kinh doanh tại Châu Âu của Palantir, đã trực tiếp gặp Tổng Tham mưu trưởng

Quân đội Thụy Sĩ Thomas Süssli tại Đối thoại Shangri-La, một hội nghị an ninh diễn ra ở Singapore vào tháng 6 năm 2024, để giới thiệu sản phẩm.

Mosley điểm lại việc quân đội Thụy Sĩ quan tâm đến việc áp dụng trí tuệ nhân tạo hoặc thuật toán vào dữ liệu, đồng thời đề xuất trình diễn thực tế các sản phẩm, bao gồm cả ứng dụng đo lường trạng thái sẵn sàng chiến đấu của các đơn vị quân đội. Bộ Tham mưu Quân đội Thụy Sĩ sau khi nhận được đề xuất này đã lập báo cáo xem xét nội bộ và báo cáo trực tiếp cho Tổng Tham mưu trưởng Süssli vào đầu tháng 12 năm 2024. Báo cáo chứa đựng sự lo ngại rằng nếu đưa các công cụ của Palantir vào sử dụng, thông tin mật của quân đội Thụy Sĩ có thể bị chuyển sang Cục Tình báo Trung ương Mỹ (CIA) và Cơ quan An ninh Quốc gia Mỹ (NSA), và quân đội Thụy Sĩ dựa trên báo cáo này đã chính thức từ bỏ kế hoạch áp dụng.

Khi sự từ chối kéo dài qua 5 cơ quan và 4 năm tích tụ lại, thái độ không chấp nhận Palantir tại Thụy Sĩ đã định hình như một nét văn hóa cơ quan. Palantir trong suốt thời gian này đã tích cực gõ cửa các cơ quan công quyền Thụy Sĩ, nhưng rốt cuộc không giành được dù chỉ một hợp đồng. Theo đưa tin của phương tiện truyền thông an ninh Gendata vào ngày 14 tháng 2 năm 2026, lý do Thụy Sĩ khước từ Palantir không phải vì năng lực kém. Cấu trúc nội bộ độc quyền và thiếu minh bạch, quyền tài phán của nước ngoài, cùng phương thức cập nhật từ xa đã được đánh giá là những rủi ro chủ quyền không thể kiểm soát.

Đánh giá từ phía Thụy Sĩ là việc giữ dữ liệu trong lãnh thổ Thụy Sĩ và đưa các điều khoản bảo vệ vào hợp đồng không đủ để ngăn chặn rủi ro này.

Palantir cũng phản ứng mạnh mẽ trước các báo cáo truyền thông đề cập đến làn sóng từ chối này. Phương tiện truyền thông điều tra Republik của Thụy Sĩ vào tháng 12 năm 2024 đã đăng hai bài báo cho rằng mối quan hệ giữa Palantir và Thụy Sĩ có thể tiềm ẩn nguy cơ. Palantir đã đệ đơn kiện Republik, yêu cầu đăng tải 23 bài phản bác lại báo cáo này. Tòa án Thương mại Zurich chỉ chấp nhận việc đăng tải duy nhất một trong số 23 bài, và khoản tiền bồi thường thiệt hại được ấn định trả cho Palantir cũng chỉ ở mức 9.000 franc Thụy Sĩ. Phán quyết này đã tạo thêm một vết nứt vào mức độ tin cậy của Palantir tại Thụy Sĩ.

Vào thời điểm tương tự, một biện pháp mới cũng xuất hiện tại Tây Ban Nha. Văn phòng Thủ tướng Tây Ban Nha đã đưa ra chỉ thị cho các doanh nghiệp nhà nước trực thuộc Công ty Cổ phần Quản lý Vốn Nhà nước (SEPI) không ký hợp đồng mới với Palantir, và thông tin này đã được truyền thông Tây Ban Nha công bố vào ngày 1 tháng 7 năm 2026. Biện pháp này nhắm đến các doanh nghiệp nhà nước xử lý mạng thông tin liên lạc cao cấp và thông tin quân sự như công ty viễn thông Telefónica, công ty quốc phòng Indra, và công ty đóng tàu Navantia. Tuy nhiên,

họ không hủy bỏ các hợp đồng đã ký kết. Hợp đồng trị giá khoảng 16,5 triệu euro mà Trung tâm Tình báo Quân đội Tây Ban Nha (CIFAS) ký với Palantir vẫn sẽ tiếp tục cho đến tháng 11 năm 2026.

Thực tế rằng việc ngăn chặn các hợp đồng mới và việc chấm dứt các hợp đồng hiện có là hai vấn đề khác nhau cũng được xác nhận tương tự qua trường hợp Tây Ban Nha.

Khi đặt Hà Lan, Thụy Sĩ và Tây Ban Nha cạnh nhau, thực tế cho thấy châu Âu không chỉ có một cách duy nhất để giữ khoảng cách với Palantir. Hà Lan không thể dễ dàng loại bỏ chương trình đã thâm nhập vào nhiều nơi trong hệ thống quốc phòng chỉ bằng ý chí chính trị. Thụy Sĩ, nhờ sự tích lũy các đánh giá từ nhiều cơ quan nhằm ngăn chặn ngay từ đầu không cho công nghệ này bước qua ngưỡng cửa, giờ đây đã đạt đến trạng thái thậm chí không cần phải thuyết phục lại. Tây Ban Nha chọn con đường đóng cửa đối với các hợp đồng trong tương lai, nhưng vẫn chờ cho đến khi các hợp đồng đã ký kết hết hạn.

Dù theo hướng nào, thực tế vẫn giống nhau: để vận hành một hệ thống an ninh mà không phụ thuộc vào công nghệ Mỹ, từng điều khoản trong hợp đồng hay từng thỏa thuận giữa các cơ quan đều phải được chuẩn bị sẵn từ trước.

---

## **Căn cứ và tài liệu tham khảo**

1. Eglė Krištopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, <https://cybernews.com/tech/dutch-defense-palantir/>
2. Tác giả không rõ, 'Defensie zoekt alternatief voor Palantir-software', Computable, 2026-06-03, <https://www.computable.nl/2026/06/03/defensie-zoekt-alternatief-voor-palantir-software/>
3. Tác giả không rõ, 'Defensie wil software Palantir "binnen twee jaar" vervangen door Europees alternatief', Nederlands Dagblad, 2026, <https://www.nd.nl/nieuws/politiek/1319116/defensie-wil-software-palantir-binnen-twee-jaar-vervangen-doo>
4. Tác giả không rõ, 'Over twee jaar exit Palantir? Voorlopig blijft het bij intenties en verkenningen', iBestuur, 2026, <https://ibestuur.nl/markt-en-overheid/inkoop-en-aanbesteding/exit-palantir-blijft-het-bij-intenties-en-verkenningen>
5. Follow the Money, 'Omstreden techbedrijf Palantir kan bij geheime data van Defensie', Follow the Money, 2026, <https://www.ftm.nl/artikelen/omstreden-techbedrijf-palantir-kan-bij-geheime-data-van-defensie>
6. Follow the Money, 'Het Nederlandse leger doet al jaren in het geheim zaken met de omstreden techreus Palantir, net als de politie', Follow the Money, 2026, <https://www.ftm.nl/artikelen/het-nederlandse-leger-doet-al-jaren-in-het-geheim-zaken-met-de-omstreden-techreus-palantir-net-als-de-politie>
7. Tác giả không rõ, 'Switzerland Ends Palantir Contract Over Data Sovereignty Risks', ZENDATA Cybersecurity, 2026-02-14, <https://zendata.security/2026/02/14/switzerland-ends-palantir-contract-over-data-sovereignty-risks/>

8. Republik, 'How tenaciously Palantir courted Switzerland', Republik, 2026-02-18, <https://www.republik.ch/2026/02/18/how-tenaciously-palantir-courted-switzerland>
9. Republik, 'Überwachungstechnologie: Wie hartnäckig Palantir die Schweiz umwarb', Republik, 2025-12-08, <https://www.republik.ch/2025/12/08/wie-hartnaeckig-palantir-die-schweiz-umwarb>
10. Tác giả không rõ, 'Switzerland rejects Palantir over fears of US access to military data', 20 Minuten, 2026, <https://www.20min.ch/story/kontroverser-it-konzern-palantir-umwarb-den-bund-jahrelang-und-blitzte-immer-wieder-ab-103466880>
11. Tác giả không rõ, 'Palantir Took a Swiss Courtroom Loss and a European Credibility Hit', Yahoo Finance, 2026, <https://finance.yahoo.com/markets/stocks/articles/palantir-took-swiss-courtroom-loss-111400896.html>
12. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, <https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns>

## 2.1 Vụ chặn 'Fable 5' của Anthropic và lời cảnh báo dành cho các đồng minh

Sự bất đồng giữa Bộ Quốc phòng Mỹ và công ty trí tuệ nhân tạo Anthropic đã âm thầm tích tụ từ trước năm 2026. Anthropic đã tự đề ra hai giới hạn khi cung cấp các mô hình trí tuệ nhân tạo của mình cho các cơ quan chính phủ. Một là mô hình của công ty không được tích hợp vào các hệ thống vũ khí trực tiếp nhắm vào con người để sát hại. Hai là mô hình không được sử dụng cho các nhiệm vụ giám sát bí mật bừa bãi nhắm vào công dân nước mình. Hai điều kiện này vốn là sự mở rộng từ chính sách sử dụng mà công ty đã làm rõ trước khi ký hợp đồng với chính phủ. Ban lãnh đạo Bộ Quốc phòng đã không chấp nhận các điều kiện này.

Họ yêu cầu quyền truy cập hoàn toàn không bị ràng buộc bởi bất kỳ hạn chế nào. Nội dung thực chất trong yêu cầu của Bộ Quốc phòng là phải có khả năng kết nối trực tiếp mô hình trí tuệ nhân tạo vào hệ thống chỉ định mục tiêu vũ khí, hoặc tích hợp không giới hạn vào hệ thống giám sát lọc thông tin liên lạc và dữ liệu vị trí của công dân nước mình. Anthropic nhận thấy nếu chấp nhận những yêu cầu này, trí tuệ nhân tạo của họ sẽ trực tiếp can thiệp vào các quyết định định đoạt sống chết của con người hoặc việc giám sát toàn diện đối với công dân trong nước. Công ty vẫn giữ vững lập trường bảo vệ bằng được hai giới hạn này, ngay cả khi phải chấp nhận rủi ro mất đi khách hàng chính phủ. Các cuộc đàm phán đã không thể đi đến thống nhất.[1]

Khi Anthropic không chịu lùi bước, Bộ Quốc phòng đã chỉ đích danh công ty này là một yếu tố đe dọa đối với chuỗi cung ứng phần mềm trong nước. Các quan chức Bộ Quốc phòng đã chính thức chỉ định Anthropic là doanh nghiệp gây rủi ro chuỗi cung ứng nghiêm trọng cho an ninh quốc gia. Việc chỉ định này vốn là một biện pháp hành chính nghiêm khắc trước đó chỉ áp dụng cho các pháp nhân thuộc các quốc gia thù địch với Mỹ. Việc một công ty trí tuệ nhân tạo tư nhân nhận phải sự chỉ định như vậy là điều hiếm thấy cho đến thời điểm đó.

Chính quyền Trump ngày 28 tháng 2 năm 2026 đã ra lệnh cấm các cơ quan chính phủ liên bang sử dụng các chương trình trí tuệ nhân tạo của Anthropic.[1] Lệnh này bề ngoài trông giống như một biện pháp hành chính xử lý các quy định mua sắm, nhưng thực chất là công cụ gây áp lực buộc Anthropic phải chấp nhận các điều kiện truy cập mà Bộ Quốc phòng mong muốn. Việc bị chỉ định là doanh nghiệp rủi ro chuỗi cung ứng không chỉ là một danh xưng mang gánh nặng về mặt tên gọi. Pháp nhân nhận sự chỉ định này sẽ bị quản lý như một nhà cung cấp

không đáng tin cậy trong hệ thống mua sắm của Bộ Quốc phòng, thường gặp khó khăn trong việc ký kết hợp đồng mới và các hợp đồng hiện có cũng bị đưa vào diện xem xét lại.

Trước đó, biện pháp này được sử dụng để sàng lọc các pháp nhân có liên quan đến những quốc gia thù địch với Mỹ. Chưa từng có công ty phát triển trí tuệ nhân tạo nổi tiếng thế giới nào ở Thung lũng Silicon bị đưa vào danh sách này cho đến lúc đó. Bản thân việc Anthropic nhận sự chỉ định này cho thấy Bộ Quốc phòng đang coi xung đột này là vấn đề mối đe dọa an ninh, thay vì một cuộc đàm phán về các điều khoản hợp đồng.

Đối mặt với áp lực này, Anthropic đã không lùi bước và vụ việc được đưa ra tòa án. Thẩm phán tòa án liên bang ngày 27 tháng 3 năm 2026 đã không phán quyết có lợi cho Bộ Quốc phòng. Thẩm phán nhận định rằng áp lực mà Bộ Quốc phòng đè lên Anthropic là hành vi trả đũa chính trị vi phạm quyền tự do ngôn luận được Tu chính án thứ nhất của Hiến pháp bảo vệ.[1] Đây là vụ việc mà một doanh nghiệp tư nhân, khi cố gắng tuân thủ các điều kiện sử dụng do chính mình đề ra, đã va chạm trực diện với quyền lực công, và sự va chạm đó đã dẫn đến phán quyết của tòa án. Phán quyết này cho thấy cơ chế kiểm soát và đối trọng đã hoạt động bên trong nước Mỹ.

Nếu áp lực mà cơ quan hành pháp gây ra đối với doanh nghiệp tư nhân bị coi là phi lý, cơ quan tư pháp có thể ngăn chặn điều đó. Tuy nhiên, sự kiểm soát tư pháp này chỉ có hiệu lực trong phạm vi lãnh thổ nước Mỹ. Cho đến thời điểm đó, đây là cuộc tranh chấp diễn ra bên trong nước Mỹ giữa cơ quan hành pháp và một doanh nghiệp tư nhân, còn các chính phủ hay cơ quan ở châu Âu không có cách nào để theo dõi cũng như không có cách nào can thiệp vào kết quả của cuộc tranh chấp này.

Mâu thuẫn nội bộ này không dừng lại ở các vụ kiện tụng trong nước. Bộ Thương mại Mỹ ngày 12 tháng 6 năm 2026 đã ra lệnh hạn chế xuất khẩu công nghệ trí tuệ nhân tạo. Bộ Thương mại đã đưa ra lý do cho biện pháp này là bảo vệ an ninh quốc gia ở cấp độ cao nhất.[2][3] Đối tượng mà lệnh này nhắm đến một cách rõ ràng là sự truy cập của người dùng mang quốc tịch nước ngoài.[2] Tuy nhiên, Anthropic không sở hữu hệ thống bộ lọc có thể phân loại quốc tịch của người truy cập theo thời gian thực. Dù một công ty cung cấp dịch vụ qua Internet có thể biết quốc gia đăng ký tài khoản hoặc quốc gia phát hành thẻ dùng để thanh toán, việc xác minh ngay lập tức quốc tịch của từng người truy cập là điều không hề dễ dàng.

Vì vậy, Anthropic đã chọn giải pháp ngắt toàn bộ truy cập Internet từ nước ngoài đối với Claude Fable 5 và Claude Mythos 5, những mô hình có hiệu suất cao nhất mà công ty sở hữu. Chỉ vài giờ sau khi lệnh được chuyển đến, kết nối của tất cả các máy tính ở nước ngoài, bao gồm cả châu Âu, đã bị ngắt.[1][5] Chỉ thị của chính phủ nhắm vào người mang quốc tịch nước ngoài, nhưng thực tế bị ngắt lại là toàn bộ kết nối ở nước ngoài, không phân biệt quốc tịch. Biện pháp lần này có tính chất khác với các lệnh trừng phạt mà Mỹ đưa một công ty hay cá nhân cụ thể vào danh sách cấm giao dịch vĩnh viễn.

Công cụ mà Bộ Thương mại sử dụng là lệnh tạm thời hạn chế xuất khẩu công nghệ cụ thể vì lý do an ninh quốc gia, và loại lệnh này về mặt pháp lý mang bản chất có thể được dỡ bỏ bất kỳ lúc nào theo quyết định chính sách, ngay cả khi được kích hoạt mà không ấn định thời hạn từ đầu. Tuy nhiên, đứng từ lập trường của các cơ quan sử dụng tại châu Âu, việc biết được sự khác biệt về mặt bản chất đó không làm giảm đi cú sốc tại thời điểm kết nối bị ngắt.

Nhiều cơ quan hành chính và viện nghiên cứu ở châu Âu đã mất đi phần mềm trí tuệ nhân tạo mà họ vẫn sử dụng hằng ngày mà không nhận được bất kỳ cảnh báo trước nào.[1][5] Không có thông báo nào giải thích lý do bị ngắt kết nối, cũng như không có kênh nào được bố trí để khiếu nại. Ngay cả với các cơ quan đã ký hợp đồng và trả phí sử dụng, tình hình cũng không có gì khác biệt. Quyền tiếp tục nhận dịch vụ hoàn toàn vô hiệu trước quyết định kiểm soát xuất khẩu của chính phủ nước chủ nhà của nhà cung cấp, thay vì dựa vào hợp đồng sử dụng. Các điều khoản dịch vụ đám mây hay thỏa thuận mức độ dịch vụ (SLA) đều không phải là cơ chế bảo vệ trước các biện pháp hành chính quốc gia thuộc loại này.

Các phương tiện truyền thông trong lĩnh vực bảo mật ở châu Âu đã đưa tin về sự cố này dưới tên gọi 'Fable-Ban'. Thực tế là chỉ một sắc lệnh hành chính của nước bạn có thể làm đình trệ mạng lưới công việc của nước đồng minh mà không có bất kỳ sự tham vấn trước nào chính là tâm điểm của các bài báo.[5]

Bên bị mất kết nối không chỉ có các bộ ngành chính phủ. Cùng với các cơ quan hành chính ở các nước châu Âu, các trường đại học và viện nghiên cứu quốc gia cũng đang sử dụng Fable 5 và Mythos 5 trong công việc hằng ngày, và các tổ chức này cũng bị mất công cụ vào cùng một thời điểm theo cùng một cách thức.[8] Sự gián đoạn mà cả khu vực công lẫn khu vực nghiên cứu học thuật cùng trải qua này đã trở thành cơ hội làm lan rộng nhận thức rằng sự cố lần này không phải là vấn đề giới hạn ở một bộ ngành hay mối quan hệ hợp đồng cụ thể nào, mà là vấn đề trải rộng trên toàn bộ các tầng lớp người dùng tại châu Âu phụ thuộc vào công nghệ Mỹ.[8] Trang blog SecureCloud, một phương tiện truyền thông về lĩnh vực

bảo mật của Đức, trong bài viết có tiêu đề về việc phần mềm Mỹ có thể được sử dụng như một vũ khí, đã đề cập đến cả những tranh cãi xung quanh Palantir lẫn vụ chặn Fable 5, đồng thời đưa ra kết luận rằng điều châu Âu cần không phải là sự không tin tưởng vào từng doanh nghiệp riêng lẻ, mà là chủ quyền số.[5] Bài viết chỉ ra rằng dù ký hợp đồng với công ty nào đi nữa, chừng nào trụ sở chính của công ty đó còn nằm ở Mỹ thì khó có thể thoát khỏi hoàn toàn cùng một rủi ro như vậy.[5]

Lệnh cấm này đã kéo dài trong 18 ngày. Phải đến ngày 1 tháng 7 năm 2026, chính phủ Mỹ mới dỡ bỏ các biện pháp hạn chế xuất khẩu.[3] Anthropic cho biết họ đã bắt đầu quy trình khôi phục quyền truy cập sau khi biện pháp kiểm soát được dỡ bỏ.[4] Theo giải thích của công ty, quyền truy cập bị gián đoạn do biện pháp ngày 12 tháng 6 không được khôi phục hoàn toàn ngay lập tức khi dỡ bỏ kiểm soát, mà diễn ra theo một tiến trình khôi phục từng bước.[4] Việc chính sách bị đảo ngược không đồng nghĩa với việc dịch vụ được bật lại ngay lập tức tại thời điểm đó. Việc tái thiết lập các kết nối bị đứt gãy cũng mất nhiều thời gian. Lệnh cấm được thực thi chỉ vài giờ sau khi lệnh được chuyển giao, nhưng việc khôi phục thì không nhanh chóng đến thế.

Cần thêm thời gian để mọi thứ trở lại trạng thái hoàn toàn như trước. Dù vậy, kết cục của sự vụ này là rất rõ ràng. Kết nối đã bị đứt, rồi sau đó được mở lại.

Có hai sự thật cần xác nhận ở đây. Thứ nhất, quyền truy cập từ nước ngoài vào Fable 5 và Mythos 5 thực sự đã bị đứt gãy. Nhiều cơ quan chính phủ và viện nghiên cứu ở châu Âu đã phải làm việc mà không có công cụ này trong 18 ngày. Thứ hai, việc phong tỏa đó không kéo dài vĩnh viễn. Chính phủ Mỹ đã thay đổi chính sách và kết nối đã được mở lại. Việc coi sự kiện này là bằng chứng cho thấy công nghệ trí tuệ nhân tạo của Mỹ sẽ không bao giờ được cung cấp cho châu Âu nữa là không đúng sự thật. Anthropic vẫn tiếp tục hoạt động kinh doanh tại châu Âu sau sự kiện, và các cơ quan châu Âu cũng tái ký hợp đồng hoặc tiếp tục duy trì các hợp đồng cũ.

Ngược lại, việc xem sự kiện này như thể không có chuyện gì xảy ra cũng không đúng thực tế. Sự gián đoạn thực tế diễn ra trong 18 ngày tuy không để lại tổn thất không thể cứu vãn, nhưng các cơ quan cần kết nối trong suốt 18 ngày đó không còn cách nào khác ngoài việc tìm phương án thay thế hoặc hoãn lại công việc. Điều mà sự kiện Fable 5 thực sự phơi bày là một cấu trúc nơi nguồn cung có thể ngừng bất cứ lúc nào, và quyền quyết định việc ngừng hay tái lập đó nằm trong tay chính phủ của nước cung cấp chứ không phải nước sử dụng. Xung đột châm ngòi cho sự kiện này ngay từ đầu vốn không nhắm vào châu Âu.

Tranh chấp giữa Bộ Quốc phòng Mỹ và Anthropic chỉ là sự kéo dài của một cuộc đàm phán mua sắm diễn ra trong nội bộ nước Mỹ, và châu Âu hoàn toàn không có liên quan gì đến cuộc đàm phán đó. Mặc dù vậy, chính phủ 및 các viện nghiên cứu châu Âu vẫn phải gánh chịu hậu quả từ kết quả của cuộc đàm phán ấy. Thực tế là công cụ làm việc có thể bị cắt đứt do dư chấn từ một xung đột chẳng liên quan đến mình đã để lại mối lo ngại thậm chí còn lớn hơn so với khi chính họ là một bên trong cuộc. Chính phủ và các cơ quan ở châu Âu không có cách nào dự đoán được lý do khiến kết nối bị ngắt theo cách tương tự lần sau sẽ là gì.

Cấu trúc này trước đó vốn là một khái niệm trừu tượng đối với các nhà hoạch định chính sách châu Âu. Cụm từ "chủ quyền kỹ thuật số" trước đây chỉ xuất hiện trong các bài tham luận hội thảo học thuật hay phần mở đầu của các báo cáo chính sách.[1] Việc một sắc lệnh kiểm soát xuất khẩu do chính phủ một nước đồng minh ban hành trong quá trình giải quyết tranh chấp chính trị nội bộ của họ có thể làm đình trệ công cụ làm việc của các cơ quan chính phủ đồng minh chỉ sau vài giờ đã không còn là lý thuyết mà trở thành thực tế đã xảy ra.[1][5] Mục tiêu lệnh của Bộ Thương mại Mỹ nhắm tới là công dân mang quốc tịch nước ngoài, nhưng hậu quả đi kèm lại là sự gián đoạn kết nối của các chính phủ và viện nghiên cứu đồng minh.

Sự lệch pha giữa mục tiêu và kết quả thực tế chính là lý do phía châu Âu tiếp nhận sự kiện này như một lời cảnh báo đặc biệt. Việc Mỹ không hề ban hành biện pháp nhắm vào châu Âu, nhưng bản thân châu Âu lại rơi vào tầm ảnh hưởng của biện pháp đó chính là vấn đề. Kiểm soát xuất khẩu của Mỹ thường là công cụ được áp dụng nhằm ngăn chặn rò rỉ công nghệ sang các quốc gia đối đầu, và theo thông lệ, các nước đồng minh bao gồm cả các quốc gia thành viên NATO luôn được tách biệt khỏi đối tượng này. Tuy nhiên, trong sự việc Fable 5, ranh giới phân biệt ấy trên thực tế đã không được duy trì.

Ranh giới phân chia giữa quốc gia đồng minh và không đồng minh chỉ tồn tại trong ý đồ chính sách, chứ không hề được hỗ trợ bởi các công cụ kỹ thuật nhằm sàng lọc quốc tịch. Điều mà các chính phủ châu Âu rút ra từ sự kiện này chính là khoảng cách đó. Khoảng trống giữa sự phân biệt trên ý tưởng và việc thực thi thực tế là điều mà vị thế đồng minh đơn thuần không thể lấp đầy.

Quốc gia hành động nhanh nhất là Pháp. Vào ngày 16 tháng 6 năm 2026, bốn ngày sau khi Bộ Thương mại Mỹ ban hành lệnh kiểm soát xuất khẩu, Bộ trưởng Nội vụ Pháp Sébastien Lecornu đã tuyên bố sẽ chuyển đổi hệ thống phân tích tình báo của Tổng cục An ninh Nội địa từ phần mềm của công ty Palantir (Mỹ) sang ArgonOS do doanh nghiệp Habsvision của Pháp phát triển.[6] Không nên hiểu

tuyên bố này đồng nghĩa với việc hợp đồng với Palantir chấm dứt ngay lập tức. Hợp đồng giữa Palantir và chính phủ Pháp tại thời điểm đó vẫn còn thời hạn nhiều năm, và việc chấm dứt đòi hỏi khoản tiền phạt vi phạm cùng các cuộc thương lượng riêng biệt.

Việc thay thế hệ thống trên thực tế cũng là một quy trình riêng biệt được tiến hành sau tuyên bố.[7] Mặc dù vậy, thực tế là chính phủ Pháp đưa ra tuyên bố theo định hướng này chỉ bốn ngày sau sắc lệnh của Bộ Thương mại đã cho thấy việc phong tỏa Fable 5 dịch chuyển sang thảo luận chính sách nội bộ ở châu Âu nhanh đến mức nào. Pháp chỉ là quốc gia đầu tiên đưa ra tuyên bố trong làn sóng này, chứ không phải quốc gia duy nhất.

Trong vài tháng sau khi Fable 5 bị phong tỏa, các chính phủ khác tại châu Âu cũng lần lượt khởi động quy trình tái kiểm tra mức độ phụ thuộc vào công nghệ Mỹ.[8] Dù con đường cụ thể mà mỗi quốc gia lựa chọn có sự khác biệt, nhưng điểm chung là sự kiện lần này chính là cột mốc khởi đầu.

Bài học mà trường hợp của Anthropic để lại cho châu Âu không phải là việc không thể tin tưởng một công ty cụ thể. Anthropic đã kiên định giữ vững các điều khoản sử dụng do mình đặt ra trước các yêu cầu của Bộ Quốc phòng, và tòa án cũng đã tuyên phần thắng cho công ty này. Áp lực mà công ty phải chịu khi nỗ lực bảo vệ hai ranh giới là vũ khí sát thương và giám sát diện rộng không phân biệt, ngược lại càng chứng minh họ đã trung thành với những nguyên tắc của chính mình. Vấn đề bị chỉ trích không phải là thái độ của Anthropic, mà là chính bản thân cấu trúc cho phép chính phủ Mỹ, một khi hạ quyết tâm, có thể ngắt dịch vụ nước ngoài của bất kỳ doanh nghiệp Mỹ nào theo cách tương tự.

Hôm nay là mâu thuẫn giữa Bộ Quốc phòng và Anthropic, nhưng lần tới một xung đột khác với một công ty khác hoàn toàn có thể dẫn đến kết quả tương tự. Điều đó đúng cho dù mâu thuẫn bắt nguồn từ tranh chấp thương mại, chính sách an ninh, hay từ đàm phán nội bộ giữa chính phủ và doanh nghiệp như lần này. Các chính phủ và viện nghiên cứu ở châu Âu không phải là bên trong cuộc xung đột, nhưng lại đứng ở vị trí phải gánh chịu toàn bộ hậu quả.

Khoảng thời gian 18 ngày không hề ngăn đối với việc ngưng trệ công việc thực tế. Đồng thời, sự kiện này cũng cho thấy giai đoạn đó rồi cũng kết thúc. Khi đánh giá của chính phủ Mỹ thay đổi, kết nối lại được mở. Lý do nhiều chính phủ châu Âu bắt đầu rà soát lại chính sách mua sắm công nghệ của nước mình sau sự việc này nằm chính ở điểm đó. Sự việc làm rõ thực tế rằng dù hợp đồng có cài cắm các điều khoản chi tiết đến đâu, những điều khoản ấy cũng không có hiệu lực trước quyết định từ chính phủ nước xuất xứ của nhà cung cấp. Việc kết nối bị đứt không

đáng ngại bằng thực tế là quyền quyết định khi nào mở hay đóng kết nối lại nằm ngoài tầm kiểm soát của chính họ, và đó mới là vấn đề còn đọng lại lâu dài.

Vì vậy, sự cố Fable 5 đã đi vào các tài liệu chính sách của châu Âu không phải với tư cách một câu chuyện về lệnh phong tỏa kéo dài vĩnh viễn, mà là câu chuyện về việc lệnh phong tỏa có thể tái diễn bất kỳ lúc nào và quyền quyết định thuộc về chính phủ của một quốc gia khác. Đây chính là lý do sự cố này tiếp tục được trích dẫn ngay cả sau khi kết nối đã được khôi phục. Câu hỏi còn lại sau khi khủng hoảng qua đi không phải là điều gì đã bị đứt gãy, mà là liệu chính phủ nước khác có thể đưa ra quyết định tương tự vào lần sau hay không. Chừng nào châu Âu chưa thể tự mình kiểm soát câu trả lời cho câu hỏi này, việc phong tỏa kéo dài 18 ngày không phải là một sự cố đơn lẻ chỉ xảy ra một lần, mà vẫn là một khả năng có thể tái diễn.

---

## Căn cứ và tài liệu tham khảo

1. Centre for Future Generations, 'Enforcement spotlight, Spring 2026', Centre for Future Generations, số mùa xuân năm 2026.
2. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, ngày 12 tháng 6 năm 2026, <https://www.anthropic.com/news/fable-mythos-access>
3. Gyana Swain, 'US reverses export restrictions on Anthropic's Fable 5, Mythos 5 AI models', Computerworld, ngày 1 tháng 7 năm 2026, <https://www.computerworld.com/profile/gyana-swain-2/>
4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, năm 2026, <https://www.anthropic.com/news/redeploying-fable-5>
5. Sebastian Deck, 'US Software as a Weapon: Palantir's Manifesto Dramatically Highlights the Need for Digital Sovereignty', SecureCloud Blog, ngày 8 tháng 6 năm 2026, <https://blog.securecloud.de/en/us-software-als-waffe-palantirs-manifest-zeigt-drastisch-notwendigkeit-digitaler-souveraenitaet>
6. Jon Henley, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, ngày 16 tháng 6 năm 2026, <https://www.theguardian.com/world/2026/jun/16/france-ai-data-tools-palantir-chapsvision>
7. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, ngày 17 tháng 6 năm 2026, [https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice\\_6754592\\_7.html](https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html)
8. 「Báo cáo phân tích về động thái rời bỏ Palantir và chủ quyền hóa kỹ thuật số của các quốc gia chủ chốt thuộc Liên minh châu Âu (EU)」, năm 2026, tr. 1-2.

## **2.2 Bẫy lập pháp ngoài lãnh thổ: Thực chất thẩm quyền tài phán của Đạo luật CLOUD và Điều 702 FISA của Mỹ**

Các quốc gia thành viên Liên minh châu Âu từ lâu đã tin rằng thông tin sẽ an toàn nếu họ đặt máy chủ dữ liệu trong lãnh thổ nước mình. Các công ty Mỹ như Amazon, Microsoft và Google cũng xây dựng các trung tâm dữ liệu ở Frankfurt, Paris hay Dublin và dùng niềm tin này làm khẩu hiệu quảng cáo. Tuy nhiên, việc máy chủ đặt trên đất châu Âu và việc thông tin bên trong máy chủ đó nằm ngoài tầm với của luật pháp Mỹ là hai chuyện hoàn toàn khác nhau. Nguyên nhân là vì hai đạo luật do Quốc hội Mỹ ban hành — Đạo luật CLOUD và Điều 702 Đạo luật Giám sát Tình báo Nước ngoài (FISA) — hoạt động dựa trên tư cách pháp nhân của công ty chứ không dựa trên biên giới quốc gia.

Để hiểu tại sao hai đạo luật này lại khiến các quan chức phụ trách mua sắm công của châu Âu căng thẳng ở thời điểm hiện tại, trước tiên cần nhìn vào bối cảnh Đạo luật CLOUD ra đời. Tháng 12 năm 2013, cơ quan điều tra liên bang Mỹ đã gửi lệnh khám xét cho Microsoft, yêu cầu giao nộp thông tin tài khoản email của một người dùng liên quan đến cuộc điều tra buôn bán ma túy. Vấn đề là dữ liệu của tài khoản đó lại được lưu trữ trên máy chủ đặt tại Dublin, Ireland. Microsoft đã đệ đơn kiện với lý do lệnh của Mỹ không có hiệu lực đối với dữ liệu nằm ngoài lãnh thổ Mỹ, và vào năm 2016, Tòa Phúc thẩm Liên bang New York đã tuyên phán thắng thuộc về Microsoft.

Trong khi Bộ Tư pháp Mỹ không đồng ý với phán quyết này và đưa vụ việc lên Tòa án Tối cao Liên bang, Quốc hội Mỹ đã thông qua Đạo luật CLOUD vào ngày 23 tháng 3 năm 2018. Vì đạo luật mới đã thay đổi chính cơ sở của vụ tranh chấp này, Tòa án Tối cao nhận thấy không cần thiết phải xét xử tiếp và đã cho khép lại vụ kiện. Đạo luật CLOUD ra đời theo cách đó, giải quyết bằng con đường lập pháp một cuộc tranh chấp mà chính phủ Mỹ suýt thua tại tòa.

Cốt lõi của đạo luật này rất đơn giản. Nó không hỏi dữ liệu được lưu trữ ở quốc gia nào. Nó hỏi liệu công ty quản lý dữ liệu đó có nằm trong thẩm quyền tài phán của Mỹ hay không. Trong thuật ngữ pháp lý, điều này được thể hiện qua ba tiêu chí: chiếm hữu, lưu giữ và kiểm soát. Nếu là một công ty có trụ sở tại Mỹ hoặc một công ty con ở nước ngoài mà công ty Mỹ nắm giữ cổ phần và quyền quản lý, thì thông tin do công ty đó chiếm hữu, lưu giữ hoặc kiểm soát phải được giao nộp

theo lệnh khám xét hoặc lệnh của tòa án Mỹ, bất kể vị trí vật lý nơi thông tin đó được lưu trữ.

Ở điểm này, cần phân biệt rõ những gì Đạo luật CLOUD thực sự cho phép làm và những gì mọi người thường hiểu lầm. Những gì Đạo luật CLOUD thực sự cho phép làm là rất rõ ràng. Các nhà cung cấp dịch vụ truyền thông hoặc nhà cung cấp dịch vụ tính toán từ xa thuộc thẩm quyền tài phán của Mỹ có nghĩa vụ pháp lý phải tuân theo yêu cầu hợp pháp của chính phủ Mỹ để giao nộp thông tin mà mình chiếm hữu, lưu giữ hoặc kiểm soát, bất kể thông tin đó nằm trên máy chủ ở quốc gia nào trên thế giới. Ngược lại, cũng có nhiều điều mà Đạo luật CLOUD không tự động hàm ý. Thứ nhất, đạo luật này không có nghĩa là chính phủ Mỹ đã nắm trong tay toàn bộ dữ liệu.

Chính phủ vẫn phải trải qua các thủ tục pháp lý chính thức như lệnh của tòa án hoặc lệnh triệu tập của viện kiểm sát trong từng vụ án riêng biệt. Thứ hai, điều đó cũng không có nghĩa là mọi yêu cầu đều tự động được chấp thuận. Đạo luật CLOUD chỉ mở ra một kênh hẹp cho phép doanh nghiệp khiếu nại lên tòa án đối với công dân của các chính phủ nước ngoài đã ký kết thỏa thuận thực thi tương hỗ chính thức với chính phủ Mỹ. Từ sau năm 2022, chỉ có hai quốc gia ký kết thỏa thuận này là Anh và Australia, còn Liên minh châu Âu vẫn chưa ký thỏa thuận như vậy với Mỹ. Vì vậy, đối với thông tin của công dân châu Âu, ngay cả thủ tục khiếu nại ngoại lệ này cũng không được áp dụng.

Ngay cả trong trường hợp của Anh, nước đã ký thỏa thuận, kênh này cũng không hề rộng mở. Tòa án chỉ chấp nhận khiếu nại nếu đối tượng bị yêu cầu không phải là công dân Mỹ và không cư trú tại Mỹ, đồng thời công ty phải chứng minh được rằng hành vi giao nộp thông tin thực sự xung đột với luật pháp Anh. Trong trường hợp không có thỏa thuận như Liên minh châu Âu, ngay cả kênh hạn chế này cũng không tồn tại. Thứ ba, phạm vi tác động của đạo luật này phụ thuộc vào quốc tịch và cơ cấu kiểm soát của công ty, chứ không phụ thuộc vào vị trí vật lý của máy chủ. Nếu là một công ty châu Âu thuần túy không có bất kỳ mối quan hệ cổ phần hay quản lý nào với Mỹ, công ty đó sẽ không thuộc đối tượng điều chỉnh của Đạo luật CLOUD.

Sẽ dễ hiểu hơn nếu theo dõi cấu trúc này qua một kịch bản cụ thể. Giả sử một cơ quan hành chính của Pháp ký hợp đồng với một công ty con tại châu Âu của một công ty Mỹ, trong đó đưa vào điều khoản bắt buộc phải lưu giữ dữ liệu trong lãnh thổ Pháp. Hợp đồng này là cam kết giữa chính phủ Pháp và công ty con tại châu Âu. Tuy nhiên, nếu công tố viên Mỹ muốn có dữ liệu đó, họ sẽ không gửi lệnh đến công ty con ở Pháp mà gửi đến công ty mẹ ở Mỹ. Vì công ty mẹ là thực thể nằm

giữ cổ phần và quyền quản lý công ty con, nên theo luật pháp, công ty mẹ được coi là ở vị trí chiếm hữu, lưu giữ và kiểm soát dữ liệu đó.

Khi công ty mẹ chỉ đạo công ty con giao nộp dữ liệu, công ty con không còn cách nào khác ngoài việc tuân theo chỉ đạo đó, bất kể hợp đồng đã ký với chính phủ Pháp. Chính phủ Pháp chỉ là một bên trong hợp đồng và không có thẩm quyền can thiệp vào quá trình chỉ đạo nội bộ này. Ngay cả khi dữ liệu chưa từng rời khỏi lãnh thổ Pháp một lần nào, quy trình này vẫn diễn ra bình thường. Đây là lý do tại sao điều kiện dữ liệu ở lại châu Âu không thể làm mất đi rủi ro pháp lý. Điều quyết định rủi ro không phải là vị trí đặt máy chủ, mà là quốc tịch và cơ cấu kiểm soát của công ty quản lý máy chủ đó.

Ở đây có thêm một tầng nữa chồng lên. Điều 48 Quy định chung về bảo vệ dữ liệu (GDPR) của Liên minh châu Âu quy định rằng ngay cả khi tòa án hoặc cơ quan hành chính nước ngoài yêu cầu chuyển giao dữ liệu cá nhân, yêu cầu đó cũng không thể được chấp thuận hoặc thực thi tại châu Âu trừ khi dựa trên một hiệp định quốc tế ký kết với Liên minh châu Âu hoặc quốc gia thành viên. Thế nhưng, như đã xem xét ở trên, giữa Mỹ và Liên minh châu Âu không hề có thỏa thuận thực thi tương hỗ theo Đạo luật CLOUD. Rốt cuộc, một công ty nhận được lệnh khám xét từ Mỹ sẽ rơi vào thế kẹt giữa hai đạo luật khác nhau.

Nếu tuân theo lệnh của Mỹ, công ty sẽ giao nộp thông tin mà không có cơ sở hiệp định quốc tế như luật Liên minh châu Âu yêu cầu; còn nếu từ chối lệnh, họ có thể phải chịu trách nhiệm về tội coi thường tòa án tại tòa án Mỹ. Xung đột này không phải là tranh luận trên giấy tờ, mà là tình thế lưỡng nan mang tính cấu trúc mà các doanh nghiệp đám mây Mỹ thực sự phải đối mặt mỗi khi ký hợp đồng với khách hàng châu Âu.

Trường hợp của Italia cho thấy tình thế lưỡng nan này sâu sắc đến mức nào. Khi xây dựng Polo Strategico Nazionale — đám mây chiến lược quốc gia dành cho hành chính công, chính phủ Italia đã thiết kế để dữ liệu chỉ nằm trong lãnh thổ Italia và khóa mã hóa cũng do cơ quan trong nước trực tiếp quản lý. Tuy nhiên, công nghệ hạ tầng thực sự vận hành đám mây chiến lược này lại là các hyperscaler Mỹ như Microsoft Azure và Google Cloud. Dù nắm giữ chìa khóa trong tay, cơ quan chức năng Italia vẫn không thể xóa bỏ hoàn toàn hạn chế căn bản rằng chính cơ chế ổ khóa được khóa bằng chìa đó lại do công ty Mỹ thiết kế và cung cấp.

Ngay cả khi đã dựng lên hai lớp lá chắn là vị trí dữ liệu và khóa mã hóa, tầng thứ ba — tức quốc tịch của công nghệ phần mềm gốc — vẫn nằm ở Mỹ.

Thực tế này đã được xác nhận không phải qua các điều khoản luật pháp trừu tượng mà bằng nhân chứng thực tế. Vào ngày 17 tháng 7 năm 2025, một giám đốc pháp lý của Microsoft đã xuất hiện và tuyên thệ trước phiên điều trần của Thượng viện Pháp. Vị này thừa nhận rằng ngay cả với dữ liệu người dùng được lưu trữ vật lý tại Paris, nếu cơ quan điều tra liên bang Mỹ yêu cầu giao nộp thông tin dựa trên Đạo luật CLOUD, công ty cũng không còn cách nào khác ngoài việc giao nộp thông tin đó mà không cần sự phê chuẩn của chính phủ Pháp.

Vào ngày 22 tháng 7 năm 2025, khi tạp chí kinh tế Forbes của Mỹ đưa tin về lời khai này, các quan chức phụ trách mua sắm công trên khắp châu Âu đã nhận được sự xác nhận bằng văn bản về một thực tế rằng, chỉ riêng chính sách đặt máy chủ trong lãnh thổ quốc gia là không đủ để thoát khỏi tầm tài phán của luật pháp Mỹ.

Một mối đe dọa khác đi kèm với Đạo luật CLOUD là Mục 702 của Đạo luật Giám sát Tình báo Nước ngoài (FISA). Điều khoản này nằm trong bản sửa đổi Đạo luật Giám sát Tình báo Nước ngoài được ban hành vào năm 2008, cho phép các cơ quan tình báo như Cơ quan An ninh Quốc gia Mỹ (NSA) thu thập dữ liệu Internet và bản ghi thông tin liên lạc của người nước ngoài ở bên ngoài lãnh thổ Mỹ mà không cần thông qua sự kiểm duyệt lệnh của tòa án cho từng đối tượng riêng lẻ. Nếu Đạo luật CLOUD là một công cụ thực thi pháp luật dựa trên các yêu cầu riêng lẻ của cơ quan điều tra, thì Mục 702 lại là quyền hạn giám sát được các cơ quan tình báo vận dụng rộng rãi dưới danh nghĩa thu thập tình báo nước ngoài. Vì điều khoản này là một đạo luật có thời hạn, nên Quốc hội Mỹ phải xem xét và gia hạn lại sau mỗi vài năm.

Vào tháng 4 năm 2024, Quốc hội Mỹ thông qua Đạo luật Cải cách Tình báo và An ninh Mỹ để tiếp tục gia hạn Mục 702, duy trì hiệu lực của điều khoản này đến tháng 4 năm 2026. Sau đó, Quốc hội đã lùi thời hạn thêm một lần nữa đến ngày 12 tháng 6, và cuối cùng đạo luật gia hạn mới đã không được thông qua trước thời điểm đó, khiến bản thân điều luật chính thức hết hiệu lực vào nửa đêm ngày 12 tháng 6 năm 2026. Tuy nhiên, Tòa án Giám sát Tình báo Nước ngoài Mỹ (FISC) đã phê chuẩn một chứng nhận giám sát có thời hạn một năm vào tháng 3 năm 2026, và chứng nhận này được thiết kế để tiếp tục duy trì hiệu lực ngay cả khi luật đã hết hạn, do đó quyền hạn giám sát thực tế vẫn tiếp tục hoạt động cho đến tháng 3 năm 2027.

Việc tồn tại sự bất hợp nhất giữa sự còn mất của điều luật và việc tiếp tục giám sát thực tế cho thấy việc kiểm soát quyền hạn này chỉ bằng một đạo luật khó khăn đến mức nào. Nhiều báo cáo truyền thông đã chỉ ra rằng mạng lưới giám sát này không chỉ bao gồm các công dân bình thường, mà còn bao gồm cả lộ trình truyền

email của các tướng lĩnh và nhà ngoại giao cấp cao thuộc các nước đồng minh. Cách thức Mục 702 thực sự hoạt động đã được tiết lộ cụ thể vào năm 2013 thông qua những tiết lộ của cựu nhân viên tình báo Mỹ Edward Snowden.

Theo các tài liệu được công bố vào thời điểm đó, Cơ quan An ninh Quốc gia Mỹ (NSA) đã căn cứ vào điều khoản này để vận hành một hệ thống thu thập có tên là PRISM, qua đó nhận trực tiếp dữ liệu của người dùng nước ngoài từ máy chủ của các công ty Mỹ như Google, Microsoft và Yahoo. Cuộc tiết lộ này là bước ngoặt khiến các quốc gia châu Âu nhìn nhận Mục 702 không phải là một điều khoản trên giấy tờ mà là một hạ tầng giám sát thực sự đang hoạt động.

Vụ án đầu tiên mà cấu trúc giám sát này xung đột trực diện tại tòa án châu Âu là phán quyết Schrems. Vào ngày 16 tháng 7 năm 2020, trong vụ kiện do công dân Áo Maximilian Schrems khởi xướng, Tòa án Công lý Liên minh Châu Âu (CJEU) đã phán quyết rằng hệ thống giám sát của Mỹ xâm phạm nghiêm trọng quyền tự quyết thông tin cá nhân của công dân châu Âu, qua đó tuyên bố thỏa thuận chuyển giao dữ liệu cá nhân giữa Mỹ và Liên minh Châu Âu mang tên Privacy Shield là vô hiệu. Điều mà tòa án phản đối không gì khác chính là các quyền hạn giám sát không cần lệnh của tòa án từ phía Mỹ như Mục 702.

Dù các doanh nghiệp châu Âu có đưa các điều khoản bảo vệ dữ liệu cá nhân chặt chẽ đến đâu vào hợp đồng, chừng nào thông tin đó còn đi qua mạng lưới thông tin liên lạc của các công ty Mỹ, bản thân hợp đồng cũng không thể ngăn cản quyền hạn giám sát của các cơ quan tình báo Mỹ; đây chính là cốt lõi của phán quyết. Ủy ban Châu Âu cũng đã chỉ ra rõ ràng Đạo luật CLOUD và Mục 702 trong báo cáo đánh giá tác động của Đạo luật Phát triển Đám mây và Trí tuệ Nhân tạo trình ngày 3 tháng 6 năm 2026, coi đây là hai lỗ hổng an ninh mang tính cấu trúc của lãnh thổ kỹ thuật số châu Âu.

Vấn đề này không dừng lại ở việc giải thích điều luật mà đã trở thành động lực làm thay đổi chính sách mua sắm công thực tế. Bộ Nội vụ bang Baden-Württemberg của Đức đã phân tích tỉ mỉ các điều kiện vận hành thực tế của Delos Cloud, một dự án đám mây công cộng dựa trên phần mềm của Microsoft. Kết quả phân tích rất rõ ràng: bản thân trung tâm dữ liệu được Văn phòng An ninh Thông tin Liên bang Đức (BSI) chứng nhận và vận hành trong lãnh thổ Đức, nhưng quyền thiết kế và kiểm soát phần mềm ứng dụng chạy trên đó vẫn nằm trong tay Microsoft của Mỹ.

Bộ Nội vụ bang kết luận rằng, chừng nào quyền kiểm soát ở tầng ứng dụng còn thuộc về công ty Mỹ, thì không thể loại trừ khả năng các cơ quan an ninh Mỹ chỉ đạo nhà cung cấp phần mềm lén lút cài đặt đường dẫn rò rỉ dữ liệu mà người dùng

không hề hay biết. Việc dữ liệu nằm trên lãnh thổ Đức về mặt vật lý cũng không thể loại bỏ nguy cơ này.

Mối quan ngại tương tự tại Hà Lan đã dẫn đến một quyết định chính thức của chính phủ. Vào tháng 11 năm 2025, Kyndryl, một tập đoàn công nghệ thông tin tổng hợp của Mỹ, đã thông báo mua lại Solvinity của Hà Lan. Solvinity là công ty vận hành hạ tầng nền tảng cho DigiD, hệ thống định danh điện tử được khoảng 16,5 triệu công dân Hà Lan sử dụng. Tại Hạ viện Hà Lan, những lo ngại liên tục nảy sinh rằng thương vụ thu mua này có thể mở đường cho quyền tài phán của Mỹ tiếp cận thông tin danh tính nhạy cảm của công dân nước mình, và chính phủ đã bắt đầu các thủ tục để ngăn chặn thương vụ.

Thứ trưởng Bộ Kinh tế Hà Lan Aarts vào ngày 26 tháng 5 năm 2026 đã thông báo chính thức ngăn chặn việc Kyndryl thu mua Solvinity với lý do phải bảo vệ lợi ích công cộng. Căn cứ mà chính phủ đưa ra rất rõ ràng: luật pháp Mỹ về mặt lý thuyết cho phép chính quyền Mỹ thu thập thông tin ngay cả khi thông tin đó được lưu trữ trên máy chủ của một công ty con ở nước ngoài do công ty Mỹ sở hữu. Đây là lần đầu tiên Cục Kiểm duyệt Đầu tư Hà Lan, được thành lập vào năm 2020, ngăn chặn việc thu mua của một doanh nghiệp Mỹ. Viện Nghiên cứu Chiến lược và Quốc tế (CSIS), một cơ quan nghiên cứu chính sách của Mỹ, đã đánh giá quyết định này là đá thử vàng để đo lường tiêu chuẩn kiểm duyệt đầu tư của các quốc gia châu Âu sẽ thay đổi như thế nào trong tương lai.

Tại Anh, vấn đề bộc lộ dưới hình thức bản thân hợp đồng trao bí mật quốc gia cho công ty Mỹ mà không phụ thuộc vào vị trí vật lý. Palantir, một công ty phân tích dữ liệu của Mỹ, đã ký hợp đồng hỗ trợ đám mây trị giá 15 triệu bảng Anh với Cơ sở Vũ khí Hạt nhân (AWE), cơ quan nghiên cứu vũ khí hạt nhân của Anh. Theo cơ quan truyền thông điều tra The Nerve khi đưa tin về hợp đồng này vào tháng 1 năm 2026, hợp đồng này không được đăng ký trên trang web công khai mua sắm chính thức của chính phủ, và Bộ Quốc phòng cũng không xác nhận hay phủ nhận sự tồn tại của hợp đồng.

Bản tin đó cũng ước tính tổng giá trị các hợp đồng mà Palantir ký với chính phủ Anh lên tới 670 triệu bảng Anh, trong đó hợp đồng với cơ sở vũ khí hạt nhân là khoản tiền nằm ngoài danh sách công khai. Ủy ban Khoa học và Công nghệ thuộc Hạ viện Anh đã chỉ ra rằng cấu trúc hiện tại phụ thuộc vào công ty Mỹ về dữ liệu y tế và mạng lưới điều tra của quốc gia là một lỗ hổng nghiêm trọng trong hệ thống mua sắm công. Thực tế là hợp đồng xử lý thông tin liên quan đến vũ khí hạt nhân bị loại khỏi danh sách mua sắm công khai một lần nữa xác nhận rằng việc ký

hợp đồng trong phạm vi biên giới vật lý không đồng nghĩa với việc quyền kiểm soát thông tin vẫn thuộc về quốc gia mình.

Ở Đức cũng xảy ra một cuộc xung đột pháp lý khác liên quan đến Palantir, nhưng cần phân biệt rằng vụ việc này là vấn đề của Hiến pháp Đức chứ không phải Đạo luật CLOUD hay Mục 702. Vào ngày 16 tháng 2 năm 2023, Tòa án Hiến pháp Liên bang Đức đã phán quyết rằng việc vận hành chương trình cảnh sát phân tích dự đoán đối với những công dân không bị nghi ngờ phạm tội là vi hiến. Hệ thống HessenDATA bị tuyên vi hiến là một chương trình an ninh trật tự được xây dựng trên nền tảng Gotham của Palantir. Điều mà phán quyết này phản đối không phải là việc áp dụng ngoại lãnh thổ của luật pháp Mỹ, mà là quyền tự quyết của công dân được Luật Cơ bản Đức đảm bảo.

Mặc dù hai vấn đề này có nguyên nhân phát sinh khác nhau, nhưng kết quả lại cùng chỉ về một kết luận: cấu trúc giao phó thông tin an ninh quốc gia cho phần mềm của công ty Mỹ, dù là do luật pháp Mỹ hay do hiến pháp nước mình, đều có thể bị lung lay đồng thời từ nhiều hướng.

Thực tế đã xác nhận rằng quyền tài phán ngoài lãnh thổ của Mỹ không chỉ dừng lại ở phạm vi yêu cầu cung cấp thông tin mà còn có thể được sử dụng như một công cụ trừng phạt. Ngày 20 tháng 8 năm 2025, Văn phòng Kiểm soát Tài sản Nước ngoài thuộc Bộ Tài chính Mỹ đã áp đặt các biện pháp trừng phạt đối với các thẩm phán của Tòa án Hình sự Quốc tế liên quan đến việc phát lệnh bắt giữ Thủ tướng Israel Netanyahu. Thẩm phán mang quốc tịch Pháp Nicolas Guillou cũng nằm trong danh sách bị trừng phạt. Sau đó, ông tiết lộ với báo chí rằng ông đã bị chặn thanh toán bằng thẻ ngân hàng và truy cập các dịch vụ của Amazon. Đã có báo cáo cho rằng tài khoản email của một quan chức Tòa án Hình sự Quốc tế khác bị trừng phạt đã bị Microsoft đình chỉ, nhưng phía Microsoft đã phủ nhận điều này.

Vụ việc này tuy dựa trên quy định trừng phạt khác với Đạo luật CLOUD hay Điều 702, nhưng cho thấy một rủi ro có cùng bản chất. Các cá nhân và tổ chức phụ thuộc vào các dịch vụ thanh toán, viễn thông và điện toán đám mây do các công ty Mỹ cung cấp có thể mất toàn bộ quyền truy cập vào các dịch vụ hàng ngày chỉ bằng một quyết định của chính quyền Mỹ.

Pháp thậm chí đã quy định rõ vấn đề này thành văn bản trong các tiêu chuẩn chứng nhận. Cơ quan An ninh Hệ thống Thông tin Quốc gia Pháp khi sửa đổi các tiêu chuẩn chứng nhận SecNumCloud cấp cho các nhà cung cấp dịch vụ đám mây tin cậy đã nêu rõ rằng điều kiện lưu trữ dữ liệu trong Châu Âu là chưa đủ. Phiên bản SecNumCloud 3.2 được sửa đổi vào năm 2025, ngoài yêu cầu trụ sở chính và

trung tâm dữ liệu của nhà cung cấp muốn được chứng nhận phải nằm trong Liên minh Châu Âu, đã bổ sung một yêu cầu mới là cơ cấu vốn và quyền biểu quyết của công ty phải hoàn toàn độc lập khỏi các luật của nước thứ ba có hiệu lực ngoài lãnh thổ như Đạo luật CLOUD.

Điều này có nghĩa là doanh nghiệp chỉ có thể nhận được chứng nhận khi thiết lập một cấu trúc mà ở đó yêu cầu tiết lộ dữ liệu từ nước thứ ba không thông qua các thủ tục tương trợ tư pháp quốc tế sẽ không thể thực thi. Việc cơ quan chức năng Pháp thực tế đã chỉ đích danh Đạo luật CLOUD trong điều khoản tiêu chuẩn chứng nhận cho thấy các nhà hoạch định chính sách Châu Âu đã xác định đây là vấn đề phải giải quyết bằng cơ cấu sở hữu của công ty chứ không phải bằng các điều khoản tin cậy trong hợp đồng.

Khi đặt những trường hợp này cạnh nhau, một kết luận rõ ràng được rút ra. Chính sách lưu trữ dữ liệu trong lãnh thổ Châu Âu là một biện pháp cần thiết, nhưng chỉ riêng điều đó thì chưa đủ. Để thực sự giảm thiểu rủi ro, chính bản thân công ty xử lý thông tin phải thoát khỏi sự sở hữu, kiểm soát và quyền thiết kế phần mềm của Mỹ. Bởi vì vị trí của máy chủ chỉ là một tọa độ trên bản đồ, còn quyền thực sự mở hay đóng dữ liệu bên trong tọa độ đó lại được quyết định bởi trụ sở chính của công ty nằm dưới sự điều chỉnh của pháp luật nước nào. Đây chính là lý do tại sao nhiều chính phủ Châu Âu đang mở rộng phạm vi thẩm định từ chủ quyền dữ liệu vật lý sang cả cơ cấu quản trị doanh nghiệp và công nghệ phần mềm gốc.

Ủy ban Châu Âu đã chuyển sự phân biệt này thành ngôn ngữ chính sách trong báo cáo đánh giá tác động của Đạo luật Phát triển Đám mây và Trí tuệ Nhân tạo. Báo cáo đánh giá đã xem xét vấn đề bằng cách chia thành ba tầng khác nhau: vị trí lưu trữ vật lý của dữ liệu, chủ thể quản lý khóa mã hóa, và cơ cấu sở hữu của công ty thiết kế và hỗ trợ phần mềm. Việc chứng nhận SecNumCloud của Pháp can thiệp vào cơ cấu vốn của công ty, hay việc Đám mây Chiến lược của Ý dù nắm giữ cả khóa mã hóa vẫn chưa thể tuyên bố độc lập hoàn toàn, đều là những ví dụ chứng minh theo cách riêng của mình rằng ba tầng này không hoạt động riêng rẽ mà phải được trang bị đồng bộ thì việc bảo vệ thực chất mới được thiết lập.

---

## **Căn cứ và tài liệu tham khảo**

1. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943 (Public Law 115-141), ngày 23 tháng 3 năm 2018. <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>
2. U.S. Congress, Foreign Intelligence Surveillance Act Amendments Act of 2008, Section 702 (Public Law 110-261), năm 2008.
3. U.S. Congress, Reforming Intelligence and Securing America Act (RISAA), ngày 20 tháng 4 năm 2024. <https://www.congress.gov/crs-product/R48592>

4. Electronic Frontier Foundation, 'Victory! 702 has Expired!', EFF Deeplinks, tháng 6 năm 2026.  
<https://www.eff.org/deeplinks/2026/06/victory-702-has-expired>
5. Court of Justice of the European Union, 'Maximillian Schrems v. Facebook Ireland Limited', Case C-311/18, phán quyết ngày 16 tháng 7 năm 2020.
6. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 48.
7. Polo Strategico Nazionale, 'Secure Public Cloud: the encrypted cloud', polostrategiconazionale.it.  
<https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/secure-public-cloud/>
8. United States v. Microsoft Corp., 584 U.S. \_\_\_\_ (2018), Tòa án Tối cao Hoa Kỳ.  
<https://supreme.justia.com/cases/federal/us/584/17-2/>
9. Emma Woollacott, 'Microsoft can't keep EU data safe from US authorities, representative admits', Forbes, ngày 22 tháng 7 năm 2025.  
<https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/>
10. European Commission, Impact Assessment accompanying the proposal for the Cloud and AI Development Act, SWD(2026) 502 final, ngày 3 tháng 6 năm 2026. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502>
11. Center for Strategic and International Studies, 'Untapping the Full Potential of CLOUD Act Agreements', CSIS Analysis. <https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements>
12. netzpolitik.org, 'Delos-Cloud: Mit Microsoft in die digitale Abhängigkeit', netzpolitik.org, năm 2024. <https://netzpolitik.org/2024/delos-cloud-mit-microsoft-in-die-digitale-abhaengigkeit/>
13. NL Times, 'Netherlands blocks U.S. takeover of DigiD operator Solvinity over security concerns', NL Times, ngày 26 tháng 5 năm 2026. <https://nltimes.nl/2026/05/26/netherlands-blocks-us-takeover-digid-operator-solvinity-security-concerns>
14. Cleary Antitrust Watch, 'Dutch Government Blocks Kyndryl's Acquisition of Solvinity in First-Ever Telecom FDI Prohibition', Cleary Antitrust Watch, tháng 6 năm 2026.  
<https://www.clearyantitrustwatch.com/2026/06/dutch-government-blocks-kyndryls-acquisition-of-solvinity-in-first-ever-telecom-fdi-prohibition/>
15. The Nerve, 'Revealed: Palantir deals with UK government amount to at least £670m – including £15m contract with nuclear weapons agency', The Nerve, tháng 1 năm 2026.  
<https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley>
16. Bundesverfassungsgericht, phán quyết liên quan đến chương trình cảnh sát dự đoán Hessendata, ngày 16 tháng 2 năm 2023.
17. Irish Times, 'It's surreal': US sanctions lock International Criminal Court judge out of daily life', Irish Times, ngày 12 tháng 12 năm 2025. <https://www.irishtimes.com/world/us/2025/12/12/its-surreal-us-sanctions-lock-international-criminal-court-judge-out-of-daily-life/>
18. Computer Weekly, 'Microsoft's ICC email block reignites European data sovereignty concerns', Computer Weekly, năm 2026. <https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns>
19. cio-online.com, 'SecNumCloud, une protection contre le droit extraterritorial, pas une garantie absolue', CIO Online, năm 2025. <https://www.cio-online.com/actualites/lire-secnumcloud-une-protection-contre-le-droit-extraterritorial-pas-une-garantie-absolue-16759.html>
20. LSTI, 'SecNumCloud Qualification (ANSSI): Audit & Evaluation', LSTI Certification.  
<https://www.lsti-certification.fr/en/Company-offers/Cybersecurity/SecNumCloud>
21. Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', The Washington Post, ngày 6 tháng 6 năm 2013.

22. Center for Strategic and International Studies, 'The Kyndryl-Solvinity Case: A Barometer for Investment Security Reviews?', CSIS Analysis, năm 2026. <https://www.csis.org/analysis/kyndryl-solvinity-case-barometer-investment-security-reviews>

## 2.3 'Air-Gap' và kiến trúc độc lập: Sự cách ly kỹ thuật vượt trên các điều khoản hợp đồng

Giám đốc phụ trách pháp lý của Microsoft đã tuyên thệ làm chứng tại phiên điều trần của Thượng viện Pháp vào tháng 7 năm 2025. Ông tuyên bố rằng ngay cả với dữ liệu người dùng được lưu trữ tại Paris, nếu các cơ quan điều tra liên bang Mỹ yêu cầu cung cấp thông tin căn cứ theo Đạo luật CLOUD, công ty cũng buộc phải giao nộp dữ liệu mà không cần sự phê chuẩn của chính phủ Pháp. Lời trần tình này đã làm rõ một sự thật đối với các quan chức hành chính Châu Âu: việc lưu giữ dữ liệu trong lãnh thổ quốc gia và việc đưa các điều khoản bảo mật vào hợp đồng là không đủ để thoát khỏi phạm vi vươn tới của quyền hạn tư pháp Mỹ.

Hợp đồng vốn dĩ là văn bản ghi lại những cam kết mà các bên giao dịch đã thỏa thuận tuân thủ. Nhiều chính phủ Châu Âu khi ký hợp đồng với các doanh nghiệp điện toán đám mây Mỹ cũng đã đưa vào các điều khoản cam kết không chuyển dữ liệu ra ngoài lãnh thổ, cũng như không bàn giao thông tin nếu không có lệnh của tòa án Châu Âu. Thế nhưng, những điều khoản như vậy chỉ phát huy tác dụng trong tình huống doanh nghiệp đối tác có thể tự do giữ trọn cam kết đó. Chừng nào doanh nghiệp ấy còn chịu sự điều chỉnh của luật pháp Mỹ, nếu chính phủ Mỹ ra lệnh cung cấp thông tin dựa trên luật nội địa của họ, doanh nghiệp sẽ buộc phải lựa chọn giữa cam kết trong hợp đồng và luật pháp nước mình, và trong hầu hết các trường hợp, họ không có lựa chọn nào khác ngoài việc tuân thủ luật pháp nước mình.

Khoảnh khắc doanh nghiệp đối tác bị ép phải lựa chọn giữa mệnh lệnh của chính phủ nước họ và cam kết trên hợp đồng, những dòng chữ trong hợp đồng không còn là tấm lá chắn bảo vệ nữa.

Sự thật này đã đánh sập một cơ chế an toàn mà nhiều quốc gia Châu Âu từng dựa vào suốt một thời gian dài. Quy định bảo vệ dữ liệu cá nhân của Liên minh Châu Âu từ lâu đã yêu cầu lưu trữ dữ liệu trong nội bộ khu vực, và nhiều cơ quan công quyền tin rằng chỉ cần máy chủ nằm trong biên giới quốc gia thì thông tin sẽ được an toàn. Yêu cầu này được gọi là sự nội địa hóa dữ liệu. Tuy nhiên, nội địa hóa dữ liệu chỉ quy định thông tin nằm ở quốc gia nào về mặt vật lý, chứ không quy định ai là người thiết kế phần mềm xử lý thông tin đó hay ai nắm quyền truy cập từ xa. Vị trí của máy chủ và quyền kiểm soát hệ thống là hai vấn đề hoàn toàn khác nhau.

Phân tích của Bộ Nội vụ bang Baden-Württemberg, Đức đã làm lộ rõ sự khác biệt này một cách cụ thể. Dự án Delos Cloud mà chính quyền bang xem xét được thiết kế theo phương thức lưu trữ dữ liệu về mặt vật lý trên các máy chủ đặt trong lãnh thổ Đức. Tuy nhiên, quyền thiết kế và cập nhật các ứng dụng thực sự vận hành điện toán đám mây này vẫn nằm trong tay trụ sở chính của Microsoft tại Mỹ. Căn cứ vào thực tế đó, Bộ Nội vụ bang kết luận rằng dù dữ liệu có nằm trên đất Đức, chừng nào quyền kiểm soát hệ thống vẫn thuộc về doanh nghiệp Mỹ thì nó vẫn không thể thoát khỏi phạm vi khám xét của Đạo luật CLOUD dù chỉ một bước.

Vấn đề không phải là dữ liệu được lưu trữ ở đâu, mà là ai thiết kế phần mềm xử lý dữ liệu đó và ai ra lệnh cập nhật.

ArgonOS, hệ thống thông tin được Pháp lựa chọn cho Tổng cục An ninh Nội địa, đưa ra câu trả lời theo một cách khác cho vấn đề mà hai trường hợp trên bộc lộ. Hapsvision, công ty phát triển ArgonOS, là một doanh nghiệp có toàn bộ cổ phần thuộc sở hữu của các cổ đông Châu Âu. Hệ thống này chỉ vận hành trong môi trường air-gap hoàn toàn ngắt kết nối với mạng dây bên ngoài, hoặc trên các máy chủ đám mây chủ quyền bị chặn truy cập từ xa. Nếu công ty sở hữu hệ thống không có pháp nhân tại Mỹ và mạng lưới đặt hệ thống không có đường dẫn nào vươn ra bên ngoài, thì cho dù cơ quan tư pháp Mỹ có phát lệnh thu thập đi nữa, bản thân con đường để thi hành lệnh đó cũng không tồn tại.

Đây là cách thức mà cấu trúc mạng và cơ cấu sở hữu tạo ra sự cách ly, chứ không phải những cam kết ghi trên hợp đồng.

Sự cách ly này còn có một khía cạnh vượt xa các biện pháp bảo vệ chính bản thân dữ liệu. ArgonOS được thiết kế để tự quản lý vòng đời của khóa mã hóa dùng để khóa dữ liệu, trong quá trình xử lý hàng chục nghìn dữ liệu có cấu trúc và phi cấu trúc thuộc nhiều loại khác nhau. Ngay cả khi dữ liệu đã được mã hóa, nếu khóa mã hóa đó do một doanh nghiệp bên ngoài quản lý, bên nắm giữ khóa vẫn có thể mở khóa bất cứ lúc nào. Việc tách biệt hoàn toàn công tác quản lý khóa mã hóa khỏi sự truy cập bên ngoài đồng nghĩa với việc giữ lại trong nước không chỉ nội dung dữ liệu mà cả quyền đọc dữ liệu đó.

Chỉ khi nắm giữ đồng thời cả vị trí máy chủ lẫn quyền giải mã thì sự cách ly mới thực sự phát huy tác dụng.

Thuật ngữ air-gap chỉ phương thức tạo ra một khoảng trống vật lý giữa mạng máy tính và mạng internet bên ngoài theo đúng nghĩa đen. Vì không có cáp kết nối, nên không có cách nào phát lệnh chặn truy cập từ xa hay cưỡng chế dừng hệ thống. Vụ việc chặn truy cập Fable 5 xảy ra vào tháng 6 năm 2026 chính là một ví

dụ nhắm trúng vào điểm này. Mô hình của Anthropic được cung cấp qua internet, và chỉ với một mệnh lệnh của Bộ Thương mại Mỹ, quyền truy cập từ nước ngoài đã bị đình chỉ hoàn toàn chỉ trong vài giờ. Nếu là dịch vụ phụ thuộc vào mạng bên ngoài, dù hợp đồng có chặt chẽ đến đâu cũng trở nên vô lực trước mệnh lệnh hành chính của quốc gia nơi đặt trụ sở chính của nhà cung cấp.

Ngược lại, nếu là một hệ thống hoàn toàn không có đường dẫn kết nối với bên ngoài, thì sẽ không có tuyến đường vật lý nào để chuyển giao mệnh lệnh đó.

Tuy nhiên, việc sở hữu kiến trúc air-gap không đồng nghĩa với việc sự an toàn được hoàn thiện ngay lập tức. Bộ Nội vụ Pháp cho biết Tổng cục An ninh Nội địa sẽ mất từ 18 đến 24 tháng để chuyển giao toàn bộ hoạt động tình báo thực chiến sang ArgonOS. Các nhân viên đã quen với giao diện thao tác của Palantir suốt hàng chục năm sẽ phải thích nghi lại với hệ thống mới, và bản thân tiêu chuẩn lưu trữ của dữ liệu tích lũy trước đây vốn được thiết kế theo hệ thống của Mỹ, dẫn đến nguy cơ thất thoát thông tin hoặc lệch định dạng trong quá trình chuyển giao. Để lấp đầy khoảng trống này, chính quyền hành chính quốc gia Pháp hứa hẹn sẽ duy trì thời kỳ quá độ vận hành song song cả hệ thống cũ và hệ thống mới cho đến năm 2027.

Giữa quyết định chuyển sang kiến trúc cách ly và thời điểm kiến trúc đó thực sự đi vào vận hành hoàn toàn luôn có một khoảng thời gian vài năm, và gánh nặng duy trì đồng thời hai hệ thống khác nhau trong vài năm đó hoàn toàn đè lên vai cơ quan tình báo.

Chi phí phải trả trong khoảng thời gian này không chỉ dừng lại ở thời hạn chuyển giao. Hệ thống bị ngắt kết nối với mạng bên ngoài cũng đồng thời bị cắt đứt khỏi các dịch vụ cập nhật thời gian thực và chia sẻ thông tin mối đe dọa mà các doanh nghiệp điện toán đám mây lớn cung cấp. Các cơ quan vận hành hệ thống độc lập như ArgonOS phải tự gánh vác việc vá lỗi bảo mật và nâng cấp tính năng bằng nhân lực của chính mình, và đây cũng là lựa chọn từ bỏ lợi thế kinh tế theo quy mô vốn được cung cấp tự động bởi mạng lưới trung tâm dữ liệu toàn cầu của các tập đoàn điện toán đám mây Mỹ.

Trong môi trường không có con đường kết nối với bên ngoài, ngay cả việc cập nhật phần mềm cũng không thể xử lý bằng cách phân phối tự động qua internet, mà trong nhiều trường hợp phải trải qua quy trình đưa vào một cách vật lý thông qua các thiết bị lưu trữ đã qua kiểm chứng. Quy trình này chậm hơn cập nhật qua internet và đòi hỏi lực lượng kiểm chứng riêng để xác minh nội dung cập nhật mỗi lần. Đó là lý do tại sao các nhà phân tích chính sách Châu Âu dù lựa chọn sự cách ly nhưng không đưa nó ra như một giải pháp vạn năng. Sự cách ly giúp ngăn chặn

mối đe dọa từ mệnh lệnh đơn phương của chính phủ nước ngoài làm đình chỉ hệ thống, nhưng đổi lại, quốc gia phải tự mình gánh vác gánh nặng bảo trì thường xuyên.

Tiêu chuẩn phân định giữa những vấn đề mà air-gap giải quyết được và không giải quyết được còn nằm ở việc hệ thống đó cần bao nhiêu tài nguyên tính toán. Các hệ thống đảm nhận việc phân tích thông tin của một cơ quan như ArgonOS có thể vận hành trong môi trường cách ly hoàn toàn chỉ với quy mô máy chủ tương đối hạn chế. Tuy nhiên, các mô hình trí tuệ nhân tạo cỡ lớn yêu cầu tính toán khối lượng khổng lồ liên tục như Fable 5 lại là câu chuyện khác. Để huấn luyện và vận hành một mô hình như vậy ngay trên lãnh thổ quốc gia trong trạng thái cắt kết nối với bên ngoài, người ta cần đến quy mô trung tâm dữ liệu, điện năng và bán dẫn vượt quá khả năng gánh vác của một cơ quan đơn lẻ.

Đây là lý do tại sao thách thức mà sự cố phong tỏa Fable 5 để lại cho châu Âu đã lan rộng từ việc tạo air-gap cho từng hệ thống riêng lẻ sang bài toán xây dựng hạ tầng tính toán ở quy mô toàn châu lục.

Phản ứng của Thụy Sĩ và Hà Lan cho thấy con đường dẫn đến sự cách ly không chỉ có một. Các cơ quan liên bang Thụy Sĩ đã từ chối đề xuất thầu của Palantir ít nhất 9 lần từ năm 2018 đến năm 2025, nhất quyết không đưa hệ thống của doanh nghiệp này vào ngay từ đầu. Khác với Pháp hay Đức, những nước phải dỡ bỏ hệ thống đã đưa vào để chuyển sang kiến trúc mới, Thụy Sĩ không phải trải qua chính quá trình chuyển đổi tốn kém đó. Bộ Quốc phòng Hà Lan đã trình Quốc hội lộ trình thay thế Palantir trong vòng 2 năm vào tháng 6 năm 2026, nhưng lộ trình này vẫn chỉ là kế hoạch, còn thời điểm hệ thống cũ thực sự bị ngắt kết nối và hệ thống mới đi vào vận hành toàn diện sẽ diễn ra sau đó.

Lựa chọn không tạo ra sự phụ thuộc ngay từ đầu và lựa chọn dỡ bỏ sự phụ thuộc đã hình thành tuy hướng đến cùng một đích đến nhưng chi phí phải trả lại khác nhau.

Trạng thái hoàn tất cách ly cũng không cố định vĩnh viễn. Khi Kyndryl, một doanh nghiệp nguồn gốc Mỹ, thông báo sẽ thôn tóm Solvinity - doanh nghiệp địa phương vốn cung cấp phần mềm cốt lõi cho mạng lưới hành chính Hà Lan, Hạ viện Hà Lan đã bày tỏ sự quan ngại sâu sắc trước thực tế rằng quyền sở hữu hạ tầng xử lý thông tin của 16,5 triệu công dân nước này có thể rơi vào tay một doanh nghiệp Mỹ chỉ sau một đêm. Dù hôm nay là hệ thống do doanh nghiệp châu Âu sở hữu, nhưng nếu ngày mai doanh nghiệp đó bị thôn tóm bởi vốn nước ngoài, sự cách ly dựa trên điều kiện cấu trúc sở hữu sẽ sụp đổ hoàn toàn.

Đây là lý do tại sao quy trình chứng minh sự cách ly không thể dừng lại ở khâu thẩm định một lần tại thời điểm đưa vào sử dụng, mà phải kéo dài thành quy trình liên tục xác minh sự thay đổi về quyền sở hữu và cấu trúc quản trị.

Ma sát do kiến trúc cách ly tạo ra cũng bộc lộ trong hợp tác quân sự xuyên quốc gia. Trong bối cảnh Ủy ban Chứng nhận An ninh Tổ chức Hiệp ước Bắc Đại Tây Dương phê chuẩn Hệ thống thông minh Maven của Palantir cho các chiến dịch vũ khí hoàn chỉnh vào ngày 22 tháng 6 năm 2026, các Tư lệnh Tối cao NATO đã chỉ trích việc từng quốc gia thành viên thực hiện các biện pháp loại bỏ Palantir trong lĩnh vực an ninh trật tự và hành chính là quyết định làm suy giảm hiệu quả trên chiến trường quân sự. Lựa chọn chuyển mạng thông tin an ninh nội địa sang ArgonOS ngắt kết nối với bên ngoài và thực tế rằng mạng thông tin mục tiêu chia sẻ giữa các lực lượng đồng minh vẫn đang vận hành trên phần mềm của Palantir đã xung đột ngay trong lòng cùng một quốc gia.

Dù cơ quan tình báo của một quốc gia hoàn tất sự cách ly trên lãnh thổ nước mình, họ cũng không thể cách ly toàn bộ mạng lưới thông tin của cả liên minh mà quốc gia đó thuộc về. Việc vạch ranh giới cách ly đến đâu vừa là bài toán kỹ thuật, vừa là lựa chọn chính trị quyết định cách thức duy trì quan hệ đồng minh.

Vẫn tồn tại khoảng cách giữa tuyên bố chính trị và sự hoàn thiện của kiến trúc. Ngay cả sau khi Bộ trưởng Lecornu tuyên bố chuyển đổi sang ArgonOS, công ty Palantir vẫn khẳng định hợp đồng hiện hữu mà họ ký với Tổng cục An ninh Nội địa vẫn có hiệu lực về mặt pháp lý. Tuyên bố của chính phủ, sự chuyển đổi quy trình mua sắm, việc chấm dứt hợp đồng trên thực tế và việc thay thế hoàn toàn hệ thống không phải là những sự kiện diễn ra đồng loạt trong cùng một ngày. Giữa thời điểm đưa ra tuyên bố chính trị và thời điểm hệ thống cũ thực sự bị ngắt kết nối vẫn còn lại một quá trình riêng biệt là đàm phán và thực thi, và trong khoảng thời gian đó, hợp đồng cũ vẫn có thể tiếp tục tồn tại trên giấy tờ.

Bản thân tuyên bố hủy bỏ hợp đồng không làm nên sự hoàn tất cách ly, và bằng chứng của sự hoàn tất không nằm ở văn bản tuyên bố mà nằm ở hệ thống cũ thực sự ngừng hoạt động cùng hệ thống mới thực sự đi vào vận hành.

Đáng chú ý là những quyết định này của Pháp và Đức đã được chính phủ mỗi nước chủ động đưa ra trước mà không chờ đợi luật pháp ở cấp độ Liên minh châu Âu được ban hành. Việc Tổng cục An ninh Nội địa chuyển sang ArgonOS cũng như lựa chọn tương tự của Cục Bảo vệ Hiến pháp Liên bang đều được thực hiện thông qua quy trình mua sắm của từng quốc gia riêng lẻ. Điều này cho thấy ngay cả trong các quy trình quen thuộc như hợp đồng và mua sắm, nếu đưa cấu trúc sở hữu và cấu hình mạng lưới của doanh nghiệp cung cấp vào làm điều kiện bắt

buộc, người ta vẫn có thể tạo ra sự cách ly thực chất. Trước khi luật pháp kịp theo sau, từng quốc gia đã chủ động thay đổi chính kiến trúc hệ thống, và nhiệm vụ tiếp theo của Liên minh châu Âu là chuyển đổi các trường hợp riêng lẻ này thành tiêu chuẩn mua sắm chung.

Ủy ban châu Âu đang nỗ lực đưa nguyên tắc cách ly này vào các quy định mua sắm thay vì phó mặc cho lựa chọn của từng doanh nghiệp riêng lẻ. Đề xuất Đạo luật Phát triển Đám mây và AI do Ủy ban châu Âu đưa ra vào tháng 6 năm 2026 vẫn chỉ là dự thảo luật cần trải qua sự thẩm tra của Nghị viện châu Âu và Hội đồng châu Âu, chứ chưa phải là luật đã được ban hành. Mặc dù vậy, đề xuất này đang định hình hướng đi yêu cầu chứng minh sự cách ly bằng chính thiết kế của hệ thống chứ không phải bằng cam kết trên hợp đồng, thông qua việc thiết lập hệ thống phân cấp thẩm định cả cấu trúc sở hữu của doanh nghiệp cung cấp, quốc tịch của Hội đồng quản trị, cho đến việc bên ngoài có quyền truy cập vào mã nguồn hay không.

Ở cấp độ cao nhất, người ta đang thảo luận về phương án yêu cầu mức độ cách ly không cho phép bất kỳ sự can thiệp nào của vốn nước ngoài trong toàn bộ quá trình thiết kế hệ thống và bảo trì mã nguồn.

Để hệ thống thẩm định như vậy có ý nghĩa, quy trình chứng minh sự cách ly không thể dừng lại ở việc tự kê khai của doanh nghiệp cung cấp. SecNumCloud, quy chuẩn chứng nhận độc lập mà Pháp vốn đã vận hành, áp dụng phương thức trong đó cơ quan thẩm định do chính phủ chỉ định sẽ định kỳ kiểm toán bản vẽ thiết kế phần mềm và mã nguồn. Không thể coi sự cách ly đã hoàn tất chỉ vì gắn cái nhãn air-gap hay đám mây chủ quyền. Chỉ khi người kiểm toán bên ngoài có thể trực tiếp xác minh sơ đồ cấu hình mạng, sổ đăng ký cổ phần sở hữu và kho lưu trữ mã nguồn, cái nhãn đó mới thực sự có thực thể.

Đề xuất Đạo luật Phát triển Đám mây và AI cũng bao hàm phương án yêu cầu chứng chỉ cấp cao nhất trong hệ thống chứng nhận do Cơ quan An ninh mạng Liên minh châu Âu vận hành, qua đó được thiết kế theo cấu trúc kép nơi chứng nhận cấp quốc gia và chứng nhận cấp liên minh cùng xác nhận sự cách ly.

Hợp đồng và kiến trúc không phải là mối quan hệ thay thế lẫn nhau mà là mối quan hệ phải vận hành cùng nhau. Hợp đồng vẫn cần thiết với tư cách là văn bản quy định giá mua sắm, chất lượng dịch vụ và trách nhiệm pháp lý. Tuy nhiên, trong các lĩnh vực như an ninh quốc gia - nơi phải ngăn chặn ngay từ đầu khả năng can thiệp của chính phủ nước ngoài - nếu sự bảo vệ mà hợp đồng cam kết không được cấu hình vật lý và cấu trúc sở hữu của hệ thống chống lưng, cam kết đó sẽ không được giữ vững vào thời điểm khủng hoảng.

Các điều khoản hợp đồng chỉ phát huy tác dụng khi đối phương có ý định giữ lời hứa. Đạo luật CLOUD và Mục 702 Đạo luật Giám sát Tình báo Nước ngoài của Mỹ đã cho thấy nhà nước vốn đã nắm quyền thu hồi ý định đó đối với các doanh nghiệp Mỹ, và sự cố phong tỏa truy cập Fable 5 đã chứng minh rằng quyền hạn đó thực sự có thể được thi hành ngay cả đối với các nước đồng minh. Lý do các cơ quan tình báo và bộ ngành hành chính của châu Âu chuyển hướng sang air-gap và cách ly cấu trúc sở hữu là bởi họ đã nếm trải thực tế rằng có một khoảng cách giữa sự bảo vệ mà văn bản hợp đồng cam kết với sự bảo vệ mà thiết kế mạng lưới thực sự tạo ra.

Việc lấp đầy khoảng trống đó không kết thúc chỉ bằng một điều khoản pháp lý, mà chỉ hoàn thành khi hội tụ đủ ba điều kiện: quá trình chuyển giao kéo dài nhiều năm, tự bảo trì và kiểm toán độc lập.

---

## **Căn cứ và tài liệu tham khảo**

1. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, ngày 17 tháng 6 năm 2026, [https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice\\_6754592\\_7.html](https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html)
2. Todd Spangler, 'Microsoft can't keep EU data safe from US authorities, representative admits', Forbes, ngày 22 tháng 7 năm 2025, <https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/>
3. Tác giả không xác định, 'Đã xác minh và tổng hợp xu hướng rời bỏ Palantir của châu Âu đến tận nguồn gốc', năm 2026.
4. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, ngày 16 tháng 6 năm 2026.
5. Loïc Duval, 'La DGSi remplace Palantir par ChapsVision', InformatiqueNews, ngày 18 tháng 6 năm 2026.
6. Tác giả không xác định, 'La DGSi prépare la sortie progressive de Palantir au profit de ChapsVision', Solutions Numériques, ngày 17 tháng 6 năm 2026.
7. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, năm 2026, <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
8. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), ngày 7 tháng 7 năm 2026.
9. Không có nguồn (bổ sung kiến thức chung). (→ Bổ sung nguyên lý kỹ thuật chung về sự khác biệt về mặt khái niệm giữa bản địa hóa dữ liệu và cách ly kỹ thuật, cũng như việc hệ thống air-gap bị ngắt kết nối khỏi sự cập nhật theo thời gian thực và hiệu ứng kinh tế theo quy mô của đám mây bên ngoài, từ đó phải gánh gánh nặng tự bảo trì.)

### 3.1 Sự khác biệt giữa lĩnh vực tình báo trong nước và lĩnh vực liên minh quân sự

Ngày 16 tháng 6 năm 2026, Thủ tướng Pháp Sébastien Lecornu tuyên bố sẽ chuyển chương trình của công ty Palantir (Mỹ) mà Tổng cục An ninh Nội địa (DGSI) sử dụng sang ArgonOS do công ty ChapsVision của Pháp phát triển. Cùng ngày, tờ Le Monde đưa tin phía Palantir khẳng định hợp đồng ký với chính phủ Pháp vẫn còn hiệu lực. Việc đưa ra tuyên bố, chấm dứt hợp đồng và thay thế hệ thống thực tế là các quy trình riêng biệt diễn ra vào những thời điểm khác nhau. Tin tức ngày 16 tháng 6 chỉ là lời tuyên bố bắt đầu quá trình chuyển đổi, chứ không phải là sự xác nhận rằng việc di chuyển sang ArgonOS đã hoàn tất.

Cơ quan Bảo vệ Hiến pháp Liên bang Đức (BfV) cũng đi theo con đường tương tự. Nhiều phương tiện truyền thông Đức đưa tin, vào tháng 5 năm 2026, BfV đã quyết định đưa ArgonOS của ChapsVision vào sử dụng thay cho phần mềm giám sát của Mỹ. Tháng 6 năm 2026, Bộ Quốc phòng Hà Lan công bố kế hoạch loại bỏ hoàn toàn phần mềm Palantir trong vòng hai năm tới. Các cơ quan liên bang Thụy Sĩ được cho là đã từ chối các hồ sơ dự thầu công nghệ thông tin của Palantir ít nhất chín lần trong khoảng thời gian từ năm 2018 đến năm 2025. Sự từ chối này của Thụy Sĩ không phải là một quyết định vội vã của một chính phủ duy nhất, mà là phán quyết mua sắm được lặp đi lặp lại qua nhiều năm.

Xu hướng tương tự cũng xuất hiện tại Tây Ban Nha. Bộ trưởng Nội vụ Fernando Grande-Marlaska đã cho dừng dự án phân tích dữ liệu mà Vệ binh Quốc gia (Guardia Civil) triển khai cùng Palantir. Hợp đồng trị giá 16,5 triệu euro do Trung tâm Tình báo Quân sự Tây Ban Nha ký kết vào năm 2023 đã không được gia hạn sau khi hết hạn. Giới lãnh đạo quân đội đã yêu cầu duy trì hợp đồng nhưng không được chấp thuận. Thay vào đó, chính phủ Tây Ban Nha quyết định đầu tư 720 triệu euro thông qua Công ty Chuyển đổi Công nghệ quốc gia để xây dựng một trung tâm dữ liệu trí tuệ nhân tạo độc lập. Chính phủ Bỉ tuyên bố sẽ đầu tư 1 tỷ euro cho đến năm 2029 để tự mình xây dựng cơ sở lưu trữ dữ liệu quân sự.

Tại Anh, xung đột còn bộc lộ gay gắt hơn. Ủy ban Khoa học, Sáng tạo và Công nghệ Hạ viện Anh đã công bố một báo cáo chỉ ra rằng cấu trúc chuyển giao mạng lưới phân tích dữ liệu công cho một doanh nghiệp tư nhân của Mỹ là một lỗ hổng an ninh. Liên quan đến hợp đồng trị giá 330 triệu bảng Anh giữa Dịch vụ Y tế Quốc gia Anh (NHS) và Palantir, các hạ nghị sĩ đã yêu cầu phải chấm dứt hợp đồng. Họ nêu ra vấn đề rằng dù trả khoản chi phí lớn như vậy nhưng chính phủ

vẫn không nhận được quyền ontology thiết kế cấu trúc dữ liệu. Điều này có nghĩa là ngay cả khi hợp đồng kết thúc, chính phủ Anh cũng không nắm giữ tài sản công nghệ nào trong tay.

Hạ viện khuyến nghị chính phủ chấm dứt quan hệ với Palantir dựa trên điều khoản quyền chấm dứt vì lý do chủ quyền có hiệu lực từ tháng 2 năm 2027. Tại Quốc hội Đan Mạch, vào tháng 5 năm 2025, phe đối lập cũng đã trình một kiến nghị chấm dứt sự phụ thuộc vào phần mềm của Mỹ.

Những quyết định này đều được đưa ra trong phạm vi một quốc gia. Các cơ quan tình báo nội địa và bộ quốc phòng có thẩm quyền tự mình quản lý hồ sơ cảnh sát và dữ liệu tình báo của nước mình. Quy trình chấm dứt hợp đồng và chuyển sang sản phẩm của công ty khác cũng có thể được tiến hành tương đối nhanh chóng trong phạm vi thẩm quyền đó. Điều này có lý do pháp lý. Đạo luật CLOUD do Quốc hội Mỹ ban hành vào tháng 3 năm 2018 quy định rằng nếu một dịch vụ do pháp nhân Mỹ kiểm soát quản lý, thì bất kể máy chủ lưu trữ dữ liệu nằm ở quốc gia nào, doanh nghiệp đó vẫn phải cung cấp dữ liệu theo yêu cầu chính thức từ cơ quan điều tra Mỹ.

Việc điều khoản này thực tế đã được áp dụng cho những vụ án nào, và liệu các yêu cầu đó có được xử lý hợp pháp trong từng trường hợp hay không là vấn đề phải đánh giá riêng biệt theo từng vụ việc. Tuy nhiên, chỉ riêng sự tồn tại của đạo luật này cũng đủ khiến các cơ quan tình báo Châu Âu coi việc dữ liệu điều tra của nước mình nằm trong hệ thống máy chủ của doanh nghiệp Mỹ là một gánh nặng.

Trong cùng thời điểm, quyết định của liên minh quân sự đa phương lại đi theo hướng ngược lại. Năm 2025, Cơ quan Thông tin và Truyền thông NATO (NCIA) trực thuộc Tổ chức Hiệp ước Bắc Đại Tây Dương (NATO) đã ký hợp đồng đưa Hệ thống thông minh Maven của Palantir vào sử dụng tại Bộ Tư lệnh Tác chiến Phối hợp. Hợp đồng này được hoàn tất chỉ trong khoảng 6 tháng, tính từ bước xác định yêu cầu cho đến khi ký kết. Hơn một năm sau đó, vào tháng 6 năm 2026, Ủy ban Chứng nhận An ninh NATO mới xác nhận khả năng tác chiến kỹ thuật hoàn toàn của hệ thống này. Thời điểm ký hợp đồng mua sắm và thời điểm được chứng nhận khả năng vận hành hoàn toàn không phải là một sự kiện duy nhất, mà ở giữa là một khoảng thời gian dài trải qua kiểm tra và thử nghiệm.

Sự khác biệt này xuất hiện là do bản thân cấu trúc công việc mà hai lĩnh vực đảm nhiệm vốn khác nhau. Hệ thống do một cơ quan tình báo nội địa sử dụng chỉ được truy cập trong phạm vi biên giới quốc gia đó và bởi các nhân viên tuân thủ pháp luật của quốc gia đó. Hồ sơ vụ án do điều tra viên của Tổng cục An ninh Nội địa Pháp lập ra được lưu trữ bằng tiếng Pháp bên trong ArgonOS, và chỉ có thể lọt ra

ngoài sau khi trải qua các thủ tục của công tố và tòa án Pháp. Trái lại, Hệ thống thông minh Maven ngay từ đầu đã được thiết kế để quân nhân từ hơn 30 quốc gia cùng nhìn vào một màn hình và chia sẻ chung một danh sách mục tiêu.

Đại tá Arnel David thuộc Quân đội Mỹ cho biết có hơn 50 ứng dụng tác chiến được phát triển bên trong hệ thống này, và các ứng dụng đó được chế tạo để tuân thủ STANAG 4774 và 4778 — các tiêu chuẩn truyền thông của lực lượng liên quân NATO. Tuân thủ tiêu chuẩn có nghĩa là tọa độ do một quân nhân Ba Lan nhập vào có thể được một quân nhân Na Uy đọc ngay lập tức, và một phi công Mỹ có thể dùng tọa độ đó để xác định đường bay. Hồ sơ điều tra nội địa chỉ an toàn khi không vượt qua biên giới, trong khi thông tin mục tiêu của tác chiến liên quân chỉ có ích khi vượt qua biên giới. Hai nhiệm vụ này có tiêu chuẩn an toàn chỉ về hai hướng hoàn toàn trái ngược nhau.

Các quan chức cấp cao nhất của NATO giải thích sự khác biệt này là một nhu cầu quân sự chứ không phải lựa chọn chính trị. Đô đốc Hải quân Pháp Pierre Vandier, Tư lệnh Tối cao Chuyển đổi của NATO, thừa nhận rằng các quân đội Châu Âu vẫn chưa có phần mềm riêng đủ tốt để tự động phân tích hình ảnh vệ tinh và điều phối việc cung ứng đạn dược. Ông cho biết không thể làm suy giảm năng lực tác chiến của liên minh trước khi công nghệ thay thế chín cồi. Các chỉ huy khác, bao gồm Tư lệnh Kai Rohrschneider, cũng cảnh báo rằng nếu các quốc gia thành viên sử dụng các hệ thống khác nhau, kết nối giữa các mạng thông tin mã hóa có thể bị đứt gãy.

Lập luận của họ là nếu một quốc gia cố gắng bảo vệ chủ quyền thông tin mà lại làm suy yếu hệ thống thông tin liên lạc của toàn bộ liên minh, thì thiệt hại gây ra sẽ còn lớn hơn.

Lập luận này cũng gặp phải sự phản bác. Lý do các quốc gia thành viên loại bỏ Palantir khỏi lĩnh vực an ninh nội địa của họ là vì luật nội địa của Mỹ trao cho cơ quan điều tra Mỹ quyền truy cập vào máy chủ của các doanh nghiệp Mỹ. Nếu mối lo ngại này được xem xét nghiêm túc trong mạng lưới tình báo nội địa nhưng lại bị bỏ qua trong hệ thống chỉ huy của NATO, thì tiêu chuẩn phân loại đó dựa trên việc bên ký hợp đồng là cơ quan trong nước hay liên minh đa quốc gia, chứ không phải dựa trên bản chất của dữ liệu.

Mâu thuẫn này cũng bộc lộ qua dòng chảy của vốn. Theo báo cáo của trang báo mạng netzpolitik.org của Đức, các ngân hàng và công ty quản lý tài sản ở nhiều nước Châu Âu thậm chí đã gia tăng quy mô mua cổ phiếu Palantir trong khi chính phủ nước họ giữ khoảng cách với công ty này. Trong báo cáo kết quả kinh doanh quý 2 năm 2026, Palantir thông báo doanh thu tăng 93 phần trăm so với một năm

trước đó. Khu vực công đã bước ra xa khỏi Palantir, trong khi vốn tư nhân lại tiến lại gần Palantir hơn trong cùng thời điểm.

Trước đó, vào ngày 16 tháng 2 năm 2023, Tòa án Hiến pháp Liên bang Đức đã ra phán quyết vi hiến đối với Hessendata, hệ thống phân tích dữ liệu tự động do cảnh sát bang Hessen xây dựng dựa trên động cơ Gotham của Palantir. Tòa án nhận định rằng không có đủ cơ sở pháp lý cho một hệ thống tự động kết hợp dữ liệu cá nhân để sàng lọc các đối tượng nguy hiểm như vậy. Phán quyết này được đưa ra trước khi Đạo luật Trí tuệ Nhân tạo của Liên minh châu Âu được ban hành, là ví dụ sớm cho thấy trật tự hiến pháp trong nước, tách biệt với ngoại lệ an ninh quốc gia, hoàn toàn có thể kiểm soát các hệ thống trí tuệ nhân tạo phục vụ trị an nội địa.

Tòa án hiến pháp của một quốc gia có thẩm quyền phanh lại hệ thống cảnh sát của chính nước mình. Tuy nhiên, trong hệ thống chỉ huy liên minh mà ba mươi hai quốc gia cùng sử dụng, không có một cơ quan đơn lẻ nào sở hữu cơ chế phanh như vậy. Sự tách rời trong lĩnh vực thông tin nội địa và sự mở rộng trong lĩnh vực liên minh quân sự rẽ nhánh từ chính sự khác biệt giữa một bên là lĩnh vực có chủ thể kiểm soát và bên kia là lĩnh vực không có.

---

## **Căn cứ và tài liệu tham khảo**

1. Ủy ban Điều tra Thượng viện Pháp, 'Báo cáo phân tích về động thái rời bỏ Palantir của các quốc gia nòng cốt trong Liên minh Châu Âu (EU) và chủ quyền kỹ thuật số', Cổng thông tin chính thức của Chính phủ Pháp, 2026.
2. John Henry, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, ngày 16 tháng 6 năm 2026.
3. Không rõ phóng viên, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, ngày 17 tháng 6 năm 2026.
4. Không rõ tác giả, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, ngày 26 tháng 5 năm 2026.
5. Ban biên tập IT-Daily, 'Palantir: Bundesamt für Verfassungsschutz wählt ChapsVision', IT-Daily, tháng 5 năm 2026.
6. Colin Bark, 'Defensie wil binnen twee jaar af van Palantir-software', ICTMagazine, ngày 3 tháng 6 năm 2026.
7. Eglé Krištopaitytė, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, ngày 2 tháng 7 năm 2026.
8. Ban biên tập Le Soir, 'Palantir s'implante en Belgique: 28 questions à (se) poser', Le Soir, ngày 19 tháng 3 năm 2026.
9. Ban biên tập Novara Media, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026.
10. Ủy ban Khoa học và Công nghệ Hạ viện Anh, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', UK Parliament, 2026.

11. Jan Ebel, 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026.
12. Palantir Investor Relations, 'Palantir Reports Q2 2026 U.S. Comm Revenue Growth of 149% Y/Y and Revenue Growth of 93% Y/Y', Palantir Technologies, 2026.
13. Tòa án Hiến pháp Liên bang Đức, 'Decisions search - Judgment of 16 February 2023', Tòa án Hiến pháp Liên bang Đức, ngày 16 tháng 2 năm 2023.
14. Không rõ tác giả, 'Tài liệu tổng hợp và xác minh nguồn gốc về xu hướng rời bỏ Palantir ở Châu Âu', 2026. (Dựa trên cơ sở Thụy Sĩ 9 lần từ chối đấu thầu và đề xuất của đảng đối lập Đan Mạch)
15. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', Thông cáo báo chí chính thức của SHAPE, ngày 30 tháng 6 năm 2026.
16. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.
17. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018.

## **3.2 NATO đạt khả năng vận hành hoàn toàn 'Hệ thống thông minh Maven (MSS)' và cái bẫy về tính tương tác**

Bộ Quốc phòng Mỹ vào năm 2017 đã khởi động Dự án Maven, sử dụng trí tuệ nhân tạo để phân tích hình ảnh từ máy bay không người lái và vệ tinh nhằm tìm kiếm các mục tiêu quân sự. Palantir đã lấy kế hoạch này làm bàn đạp để tạo ra một phiên bản thương mại, và phiên bản thương mại này chính là gốc rễ của Hệ thống thông minh Maven mà NATO đã đưa vào sử dụng.

Cơ quan Thông tin và Truyền thông NATO (NCIA) vào năm 2025 đã ký hợp đồng với Palantir để sử dụng hệ thống này tại Bộ Tư lệnh Tác chiến Liên hợp. Thời gian kéo dài từ giai đoạn xác định các yêu cầu thu mua cho đến thời điểm ký hợp đồng là khoảng 6 tháng. Tại thời điểm này, những gì NATO giành được là quyền sử dụng hệ thống và hợp đồng, chứ không phải là chứng nhận có thể sử dụng bất kỳ lúc nào trong mọi hoạt động quân sự.

Chứng nhận khả năng tác chiến kỹ thuật hoàn toàn, tức FOC (Full Operational Capability), đã ra đời hơn một năm sau đó. Ngày 22 tháng 6 năm 2026, Ủy ban Chứng nhận An ninh NATO xác nhận rằng Hệ thống thông minh Maven đã đạt đến mức có thể vận hành trên mạng bảo mật. Quyền Giám đốc Vận hành Bart van Meert của NCIA vào ngày 26 tháng 6 đã báo cáo kết quả chứng nhận này tới bộ tư lệnh các nước đồng minh. Bộ Tư lệnh Tối cao NATO (SHAPE) vào ngày 30 tháng 6 chính thức tuyên bố rằng hệ thống này có thể được sử dụng không hạn chế trong mọi lĩnh vực hoạt động quân sự, bao gồm cả huấn luyện và chiến đấu thực tế.

Tổng Giám đốc Dylan Brown của NCIA cho biết ông tự hào về sự hợp tác đã bàn giao năng lực này cho các chiến sĩ liên quân.

Giữa năm 2025 khi ký hợp đồng và năm 2026 khi chứng nhận vận hành hoàn toàn đã có một thời gian kiểm chứng. Hệ thống này đã trải qua tình huống tương tự chiến đấu thực tế trong cuộc tập trận đa quốc gia Steadfast Deterrence kết thúc tại Na Uy vào ngày 13 tháng 5 năm 2026. Thiếu tướng Rupprecht von Butler thuộc Quân đội Liên bang Đức cho biết trong cuộc tập trận này, ông đã xác nhận hiệu suất của trí tuệ nhân tạo trong việc tự động tạo ra các kịch bản hành động của quân địch giả định.

Hệ thống thông minh Maven thu thập và phân tích theo thời gian thực dữ liệu do vệ tinh quân sự, máy bay không người lái và radar gửi về. Quân nhân nhìn vào màn hình này có thể rút ngắn đáng kể thời gian chọn lọc mục tiêu oanh kích. Đại tá Arnel David của Quân đội Mỹ cho biết có hơn 50 ứng dụng tác chiến được phát triển bên trong hệ thống này, và các chương trình này được tạo ra để tuân thủ STANAG 4774 và 4778, vốn là các chuẩn truyền thông của liên quân. Việc tuân thủ chuẩn này có nghĩa là quân đội các nước thành viên có thể trao đổi an toàn thông tin mục tiêu với quân đội các nước khác.

Phía Palantir đã đưa ra lập trường rõ ràng về vấn đề quyền sở hữu dữ liệu. Fiona Bradley, người được cử đến từ Palantir, cho biết quyền sở hữu đối với toàn bộ phần mềm và dữ liệu bên trong Hệ thống thông minh Maven thuộc về liên minh NATO, đồng thời khẳng định công ty của bà không phải là một công ty tự ý xử lý rồi bán lại dữ liệu của khách hàng. Lời giải thích này trả lời cho câu hỏi dữ liệu thuộc về ai, nhưng không phải là câu trả lời cho một câu hỏi khác: ai là người thiết kế cấu trúc của chương trình xử lý dữ liệu đó.

Quyền chỉnh sửa mã nguồn cốt lõi và hệ thống phân loại dữ liệu của hệ thống, tức ontology, vẫn thuộc về đội ngũ kỹ thuật viên tư nhân của Palantir. Tọa độ mục tiêu do quân nhân các nước thành viên NATO nhập vào tuy là tài sản của liên minh theo hợp đồng, nhưng phương thức sắp xếp và phân loại các tọa độ đó chỉ vận hành trong khuôn khổ do Palantir quy định. Nếu ví như một thư viện, cấu trúc này tương tự như việc quyền sở hữu sách thuộc về thư viện, nhưng ngôi ở vị trí thủ thư quyết định xếp sách theo thứ tự phân loại nào vẫn là nhân viên của Palantir. Quyền sở hữu dữ liệu và quyền thiết kế hệ thống không phải là cùng một loại chủ quyền; những gì NATO nắm giữ là vé trước, còn vé sau vẫn nằm lại bên trong Palantir.

Hiệu suất của hệ thống này đã bước lên bàn thử nghiệm trong các chiến dịch thực tế. Quân đội Mỹ vào tháng 2 năm 2026 đã chuẩn bị cho các cuộc không kích nhắm vào các nhóm vũ trang có liên hệ với Iran. Quân đội đã vận hành Hệ thống thông minh Maven trong 24 giờ đầu tiên sau khi bắt đầu không kích và sàng lọc ra hơn 1.000 điểm mục tiêu tấn công tiềm năng. Theo dõi kết quả này, các chỉ huy liên quân đã thể hiện sự tin tưởng vào tốc độ xử lý của phần mềm Mỹ.

Cùng thời điểm đó, Pháp, Đức và Hà Lan lại đưa ra những quyết định hoàn toàn trái ngược ở phạm vi trong nước. Ngày 16 tháng 6, Pháp tuyên bố sẽ chuyển phần mềm của Tổng cục An ninh Nội địa sang ArgonOS, và Cơ quan Bảo vệ Hiến pháp Liên bang Đức cũng đưa ra quyết định tương tự vào tháng 5. Tháng 4, Phó Đề đốc Thomas Daum của Quân đội Liên bang Đức đã loại Palantir khỏi quy cách thu mua

cuối cùng của dự án điện toán đám mây quốc phòng. Trong khi cấp chỉ huy thượng tầng của NATO tiến sâu hơn vào hệ thống của Palantir, thì mạng lưới tình báo nội địa và thu mua quốc phòng của chính các quốc gia này lại đang bước ra xa hơn khỏi công ty đó.

Chuyển động theo hai hướng này đã gây ra ma sát trong nội bộ NATO. Tư lệnh Vandier thừa nhận rằng quân đội châu Âu vẫn chưa có phần mềm riêng tương đương với Palantir trong việc phân tích hình ảnh vệ tinh hay điều phối cung ứng đạn dược. Ông cho rằng không thể làm suy giảm năng lực tác chiến của liên minh trước khi công nghệ thay thế chín muồi. Tư lệnh Kai Rohrschneider của Đức cảnh báo rằng nếu mỗi quốc gia thành viên sử dụng riêng một hệ thống do nước mình tự phát triển, nguy cơ mất kết nối giữa các mạng thông tin mã hóa sẽ xuất hiện.

Để đối phó với điều này, Pháp đã bắt đầu thử nghiệm phương án thay thế của riêng mình. Tháng 6 năm 2026, Bộ Quốc phòng Pháp đã thử nghiệm nền tảng Arcadia tại một cuộc tập trận thu mua diễn ra ở Ba Lan. Arcadia là phần mềm nhận thức chiến trường do các doanh nghiệp quốc phòng Pháp gồm Thales, Safran và Mistral AI hợp tác tạo ra. Tướng Patrick Justel, Phó Tham mưu trưởng Quân đội Pháp, chỉ ra rằng thông lệ của NATO khi chấp nhận các hệ thống nước ngoài mà không có sự nghi ngờ đáng kể đang đe dọa an toàn thông tin của nước này. Lãnh đạo Pháp và Đức vào ngày 17 tháng 7 năm 2026 đã ký tuyên bố chung về việc xây dựng một khung xương sống kỹ thuật số chủ quyền của chính châu Âu.

Sẽ mất thời gian để Arcadia khẳng định vị thế đủ để thay thế Hệ thống thông minh Maven. Trong thời gian đó, yêu cầu về tính tương tác của hệ thống chỉ huy NATO sẽ tiếp tục sức ép buộc các quốc gia thành viên chia sẻ thông tin mục tiêu và tuân thủ các chuẩn truyền thông, và sức ép đó kéo việc thu mua về phía hệ thống của Palantir vốn đã được kiểm chứng và đáp ứng tiêu chuẩn. Các cơ quan tình báo nội địa có thể đưa ra quyết định và chấm dứt hợp đồng trong phạm vi biên giới quốc gia, nhưng một hệ thống chỉ huy do 32 quốc gia cùng sử dụng thì một quốc gia không thể tự ý thay đổi. Sự khác biệt này là lý do tại sao tính tương tác vẫn tiếp tục áp đảo quyền kiểm soát nội địa trong nội bộ NATO.

---

## **Căn cứ và tài liệu tham khảo**

1. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.
2. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', thông cáo báo chí chính thức của SHAPE, ngày 30 tháng 6 năm 2026.
3. Tamara Rozouvan, 'Maven Smart System achieves full operating capability with NATO', Janes, ngày 1 tháng 7 năm 2026.

4. Nuray Taylor, 'NATO's 'Digital Lethality Branch' Breaks Records in Drive for Alliance-Wide Interoperability', AFCEA International, ngày 31 tháng 7 năm 2026.
5. Fernando Castro de Beiro, 'Foreign software, Europe's War: How Maven and Palantir are already making decisions for Europe', DigitalShield, ngày 15 tháng 7 năm 2026.
6. Wikipedia, 'Palantir', hiệu chỉnh lần cuối ngày 9 tháng 8 năm 2026.
7. Phóng viên khuyết danh, 'Spain blacklists Palantir over domestic security concerns', The Cradle, ngày 3 tháng 8 năm 2026.
8. Eglė Krištopaitytė, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, ngày 2 tháng 7 năm 2026.
9. T.Wiegold, 'Cyber-Kommandeur der Bundeswehr lehnt Software von Palantir ab', Augen geradeaus!, ngày 28 tháng 4 năm 2026.
10. Ban biên tập Cybernews, 'France and Germany to build an alternative to Palantir', Cybernews, ngày 20 tháng 7 năm 2026.
11. John Henry, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, ngày 16 tháng 6 năm 2026.
12. Tác giả khuyết danh, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, ngày 26 tháng 5 năm 2026.

### **3.3 Điều khoản ngoại lệ về an ninh trong Đạo luật Trí tuệ Nhân tạo (AI Act) của Liên minh Châu Âu và điểm mù trong kiểm soát**

Đạo luật Trí tuệ Nhân tạo (AI Act) là đạo luật điều chỉnh mức độ quản lý tùy theo quy mô rủi ro mà hệ thống trí tuệ nhân tạo có thể gây ra cho con người. Hệ thống có rủi ro càng lớn thì nghĩa vụ về tính minh bạch, đánh giá rủi ro và sự giám sát của con người càng nặng nề. Điều 2 của quy định này xác định rằng đạo luật không áp dụng cho các hệ thống trí tuệ nhân tạo được đưa ra thị trường hoặc sử dụng duy nhất cho mục đích quân sự, quốc phòng và an ninh quốc gia. Ngoại lệ này không phân biệt chủ thể sản xuất hay vận hành hệ thống là cơ quan chính phủ hay doanh nghiệp tư nhân. Đoạn mở đầu (Recital) 24 nêu rõ căn cứ cho điều này.

Theo đó, an ninh quốc gia là lĩnh vực thuộc trách nhiệm đơn phương của từng quốc gia thành viên trong khuôn khổ các hiệp ước Liên minh Châu Âu, còn các hoạt động quân sự và quốc phòng do bản chất của chúng nên chịu sự điều chỉnh riêng theo Chính sách Đối ngoại và An ninh Chung của Liên minh Châu Âu.

Điều khoản ngoại lệ này không phải là một sơ hở vô tình còn sót lại trong quá trình đàm phán, mà là kết quả do các quốc gia thành viên tích cực yêu cầu và đạt được. Theo báo cáo số mùa xuân năm 2026 của Centre for Future Generations, Pháp đã cùng với Ý và Thụy Điển dẫn đầu các hoạt động vận động hành lang nhằm mở rộng phạm vi ngoại lệ dựa trên lý do an ninh quốc gia. Các chính phủ này muốn cơ quan hành pháp không phải trải qua quy trình đánh giá rủi ro của Brussels khi sử dụng camera nhận diện khuôn mặt hoặc các công cụ giám sát sinh trắc học tại nơi công cộng. Kết quả là mạng lưới thông tin của cơ quan an ninh nội địa và hệ thống nhận diện mục tiêu của liên minh quân sự đã song song nằm ngoài phạm vi áp dụng của Đạo luật Trí tuệ Nhân tạo.

Các hệ thống tiêu biểu nằm trong điểm mù này là chương trình dòng Gotham dùng cho an ninh nội địa và hệ thống Maven Smart của NATO. Các nghĩa vụ về tài liệu hóa, quy trình truy xuất sự cố và thiên vị, cũng như cơ chế để con người xem xét quyết định cuối cùng mà Đạo luật Trí tuệ Nhân tạo yêu cầu đối với các hệ thống rủi ro cao khác đều không bị bắt buộc về mặt pháp lý đối với hai hệ thống này. Quy trình mà Ủy ban Chứng nhận An ninh NATO cấp chứng nhận vận hành

hoàn toàn cho hệ thống Maven Smart vào tháng 6 năm 2026 đã không qua sự thẩm định của đạo luật này.

Tuy nhiên, sự miễn trừ này không đồng nghĩa với việc không có quản lý. Ngoại lệ ở Điều 2 chỉ giới hạn trong trường hợp được sử dụng duy nhất cho mục đích quân sự, quốc phòng và an ninh quốc gia. Ngay cả với cùng một loại phần mềm do cùng một công ty sản xuất, nếu được dùng cho các lĩnh vực không phải quân sự như hành chính công hay an ninh dân sự, phần mềm đó vẫn chịu sự điều chỉnh của Đạo luật Trí tuệ Nhân tạo. Ngoại lệ không phải là tấm nhãn gắn cho một doanh nghiệp hay khách hàng cụ thể, mà là điều kiện đi kèm với mục đích sử dụng thực tế của trí tuệ nhân tạo đó.

Không phải là không có cơ chế pháp lý nào khác ở khoảng trống mà Đạo luật Trí tuệ Nhân tạo bỏ qua. Tòa án Hiến pháp Liên bang Đức vào ngày 16 tháng 2 năm 2023, ngay cả trước khi Đạo luật Trí tuệ Nhân tạo được ban hành, đã tuyên bố hệ thống phân tích dữ liệu tự động HessenDATA của cảnh sát bang Hessen là vi hiến. Phán quyết này đã thiết lập nguyên tắc rằng ngay cả những hệ thống trí tuệ nhân tạo lấy lý do an ninh quốc gia hay trật tự trị an cũng phải có cơ sở pháp lý riêng trong trật tự hiến pháp của mỗi nước. Ngoại lệ an ninh quốc gia của Đạo luật Trí tuệ Nhân tạo chỉ có nghĩa là bản thân quy định này không áp dụng, chứ không có nghĩa là hiến pháp, pháp luật bảo vệ thông tin cá nhân và quyền giám sát của quốc hội tại các quốc gia thành viên đều biến mất.

Ở cấp độ NATO, đây cũng không phải là vùng hoàn toàn không có luật pháp. Việc hệ thống Maven Smart phải trải qua sự phê duyệt của Ủy ban Chứng nhận An ninh NATO cho thấy quy trình chứng nhận riêng của NATO đã thay thế vào chỗ mà Đạo luật Trí tuệ Nhân tạo bỏ qua. Tuy nhiên, quy trình chứng nhận này là thủ tục xác nhận việc hệ thống có hoạt động an toàn theo tiêu chuẩn quân sự hay không, chứ không được thiết kế theo các tiêu chuẩn như kiểm tra thiên vị hay nghĩa vụ minh bạch đối với công dân mà Đạo luật Trí tuệ Nhân tạo yêu cầu. Chỉ có chủ thể và tiêu chuẩn giám sát thay đổi, chứ bản thân sự giám sát không hề biến mất.

Tuy nhiên, khi sự giám sát đó bị đặt dưới chế độ bí mật quốc phòng, kênh để công dân tiếp cận xem xét kết quả đã trở nên hẹp hơn rất nhiều so với lĩnh vực thông tin nội địa.

Tháng 1 năm 2026, Nghị viện Châu Âu đã bỏ phiếu thông qua nghị quyết về chủ quyền công nghệ nhằm giảm sự phụ thuộc vào một số ít doanh nghiệp công nghệ Mỹ. Các nghị sĩ đã đưa ra lý do về rủi ro rằng nếu dữ liệu tập trung quá mức vào các tập đoàn Mỹ như Microsoft và Amazon, chỉ một quyết định của chính phủ Mỹ

cũng có thể làm gián đoạn các dịch vụ tại Châu Âu. Chính quyền Mỹ đã phản đối động thái quản lý này của Châu Âu và ám chỉ khả năng trả đũa thương mại.

Ngày 17 tháng 7 năm 2026, lãnh đạo Pháp và Đức đã ký tuyên bố chung về việc xây dựng xương sống kỹ thuật số chủ quyền của riêng Châu Âu. Hướng đi mà tuyên bố này chỉ ra là việc thực sự hoàn thiện phần mềm riêng như Arcadia. Ngoại lệ an ninh quốc gia trong Đạo luật Trí tuệ Nhân tạo là điều khoản thừa nhận thực tế rằng Châu Âu không thể ngăn chặn tình trạng phụ thuộc vào công nghệ Mỹ bằng các quy định quản lý, chứ không phải điều khoản giải quyết sự phụ thuộc đó. Việc lấp đầy khoảng trống mà bàn tay quản lý không chạm tới đã trở thành nhiệm vụ của các công nghệ thay thế do chính Châu Âu tạo ra.

---

## **Căn cứ và tài liệu tham khảo**

1. Regulation (EU) 2024/1689, Artificial Intelligence Act, Article 2 and Recital 24, ngày 13 tháng 12 năm 2024.
2. Centre for Future Generations, 「Enforcement spotlight - Spring 2026」, Centre for Future Generations, số Mùa xuân năm 2026, trang 2-3.
3. Tòa án Hiến pháp Liên bang Đức, 'Decisions search - Judgment of 16 February 2023', Tòa án Hiến pháp Liên bang Đức, ngày 16 tháng 2 năm 2023.
4. Ủy ban Điều tra Thượng viện Pháp, 'Báo cáo phân tích về động thái rời bỏ Palantir và chủ quyền số của các quốc gia chủ chốt trong Liên minh Châu Âu (EU)', Cổng thông tin chính thức của Chính phủ Pháp, 2026.
5. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', Thông cáo báo chí chính thức của SHAPE, ngày 30 tháng 6 năm 2026.
6. Bộ Quốc phòng Hà Lan và Ủy ban Công nghệ Châu Âu, 'Tài liệu tổng hợp xác minh từ nguồn gốc xu hướng rời bỏ Palantir của Châu Âu', 2026.

## **4.1 Đạo luật Phát triển Điện toán đám mây và AI (CADA) cùng đổi mới quy định tại các khu vực tăng tốc trung tâm dữ liệu**

Ủy ban Châu Âu đã chính thức đưa ra đề xuất Đạo luật Phát triển Điện toán đám mây 및 AI (Cloud and AI Development Act) vào ngày 3 tháng 6 năm 2026. Tên tiếng Anh của đề xuất này là Cloud and AI Development Act, gọi tắt là CADA. Mã số văn bản là COM(2026) 502. Cần làm rõ thực tế này trước tiên: CADA vẫn chưa phải là một đạo luật chính thức. Đây là đề xuất quy định do Ủy ban Châu Âu trình lên Nghị viện Châu Âu và Hội đồng Châu Âu để thẩm định, và tính đến thời điểm ngày 11 tháng 8 năm 2026 được đề cập trong cuốn sách này, nó vẫn chưa được chính thức thông qua.

Tại Liên minh Châu Âu, Quy định (Regulation) khác với Chỉ thị (Directive) ở chỗ nó là một hình thức pháp lý có hiệu lực mạnh mẽ, phát huy tác dụng trực tiếp mà không cần qua lập pháp riêng của nghị viện các quốc gia thành viên. Chính vì vậy, quy trình thẩm định để chốt thành quy định cũng rất nghiêm ngặt. Trong quy trình lập pháp thông thường, Nghị viện Châu Âu và Hội đồng Châu Âu phải lần lượt đưa ra các bản sửa đổi và qua các đợt bỏ phiếu thì các điều khoản mới được ấn định. Trong quá trình đó, các điều khoản và con số nằm trong bản đề xuất hiện tại hoàn toàn có thể thay đổi. Các nội dung được giải thích trong chương này như 4 mức độ bảo đảm chủ quyền, khu vực tăng tốc và điều khoản quyền chấm dứt hợp đồng đều mới chỉ là bản thiết kế ở giai đoạn đề xuất. Chúng chưa phải là những quy phạm có hiệu lực ràng buộc đối với chính phủ và doanh nghiệp các nước thành viên.

Sự phân biệt này cũng rất cần thiết để tránh nhầm lẫn CADA với Đạo luật Trí tuệ Nhân tạo của Liên minh Châu Âu (AI Act, Regulation (EU) 2024/1689). Đạo luật Trí tuệ Nhân tạo là quy định đã được ban hành và có hiệu lực từ năm 2024, phân loại các hệ thống trí tuệ nhân tạo theo mức độ rủi ro và áp đặt các nghĩa vụ tương ứng. Ngược lại, CADA là một đề xuất riêng biệt giải quyết vấn đề cơ sở hạ tầng và quy trình mua sắm công để trí tuệ nhân tạo vận hành, và tính đến tháng 8 năm 2026 vẫn chưa được ban hành. Không nên coi địa vị pháp lý của hai văn bản này là như nhau chỉ vì tên của cả hai đều chứa từ trí tuệ nhân tạo.

Một bên là quy phạm đã được thực thi, còn bên kia là đề xuất vẫn đang chờ thẩm định.

CADA xuất hiện như một phần trong Kế hoạch hành động Lục địa AI mà Ủy ban Châu Âu thúc đẩy. Mục tiêu của kế hoạch này được tóm tắt ở hai điểm: gia tăng năng lực tính toán của các trung tâm dữ liệu nằm trong lãnh thổ Châu Âu, và bảo vệ năng lực tính toán đó khỏi tài quyền tư pháp bên ngoài Châu Âu. Bối cảnh khiến hai mục tiêu này được gộp chung vào một dự luật nằm ở cấu trúc thị trường điện toán đám mây Châu Âu. Nhiều báo cáo ngành chỉ ra rằng ba công ty Amazon, Microsoft và Google chiếm thị phần áp đảo trên thị trường dịch vụ hạ tầng đám mây Châu Âu, trong khi thị phần của các doanh nghiệp có trụ sở tại Châu Âu lại thấp hơn rất nhiều.

Trong một bài viết ngày 15 tháng 6 năm 2026, tạp chí chính sách công nghệ Tech Policy Press đã chỉ ra rằng sự thiên lệch này dẫn đến lỗ hổng an ninh, đặt số phận của các hệ thống công dưới quyền tài phán của nước ngoài.

Trước CADA, Châu Âu cũng từng có nỗ lực tương tự. Dự án Gaia-X do Pháp và Đức khởi xướng vào năm 2019 là một dự án do khu vực tư nhân dẫn dắt nhằm xây dựng tiêu chuẩn hạ tầng dữ liệu mà các doanh nghiệp Châu Âu có thể dùng chung. Tuy nhiên, Gaia-X chỉ là một diễn đàn tự nguyện không có hiệu lực ràng buộc pháp lý, và với những xung đột lợi ích giữa các doanh nghiệp tham gia, dự án này bị đánh giá là không đạt được kết quả như mục tiêu ban đầu. Điểm khác biệt của CADA so với Gaia-X nằm ở chỗ nó muốn tác động trực tiếp lên chính thị trường mua sắm công bằng một quy định có hiệu lực ràng buộc pháp lý chứ không phải thông qua các tiêu chuẩn tự nguyện.

Tuy nhiên, vì quy định đó chỉ thực sự có hiệu lực khi vượt qua vòng thẩm định của Nghị viện Châu Âu và Hội đồng Châu Âu, CADA hiện tại vẫn chỉ dừng lại ở giai đoạn thể hiện ý chí.

Câu chuyện này có thể khá xa lạ với độc giả phổ thông. Một hệ thống máy tính do chính phủ, bệnh viện hay cảnh sát sử dụng không nhất thiết phải vận hành bên trong các tòa nhà nằm trong biên giới quốc gia đó. Khi thuê dịch vụ đám mây của các công ty như Amazon, Microsoft hay Google, việc tính toán thực tế sẽ diễn ra tại các khu phức hợp máy chủ cỡ lớn được các công ty này xây dựng trên khắp thế giới. Trong ngành, những khu phức hợp máy chủ siêu lớn như vậy được gọi là các hyperscaler. Ngay cả khi tòa nhà máy chủ nằm trên đất Châu Âu về mặt vật lý, nếu công ty sở hữu và vận hành tòa nhà đó là một pháp nhân Mỹ, các yêu cầu pháp lý của chính phủ Mỹ vẫn có thể can thiệp đến dữ liệu nằm trên đó.

Khoảng cách giữa vị trí vật lý và quyền kiểm soát pháp lý có thể khác nhau chính là luận điểm cốt lõi xuyên suốt toàn bộ chương này.

Bên cạnh đó, trong ngành điện toán đám mây còn có hiện tượng được gọi là trọng lực dữ liệu. Một khi lượng lớn dữ liệu đã được chuyển sang đám mây của một công ty nhất định, việc đặt các chương trình và dịch vụ xử lý dữ liệu đó vào cùng một đám mây sẽ trở nên nhanh hơn và rẻ hơn. Điều này có nghĩa là theo thời gian, dữ liệu và các ứng dụng xử lý dữ liệu đó ngày càng gắn kết sâu hơn vào hệ sinh thái của một công ty duy nhất. Không hiếm trường hợp các cơ quan công quyền ban đầu chỉ ký hợp đồng thuê dung lượng lưu trữ, nhưng chỉ sau vài năm, toàn bộ công việc hành chính đã rơi vào tình trạng không thể vận hành nếu thiếu đám mây của công ty đó.

Đây chính là lý do vì sao các nhà hoạch định chính sách Châu Âu lo ngại về độ sâu của sự ràng buộc này hơn là các con số thị phần thuần túy.

Báo cáo về sức cạnh tranh do cựu Chủ tịch Ngân hàng Trung ương Châu Âu Mario Draghi trình lên Liên minh Châu Âu vào tháng 9 năm 2024 thường được trích dẫn như một văn bản cảnh báo trước về vấn đề này. Báo cáo Draghi khuyến nghị rằng để Châu Âu có thể tự chủ phát triển trí tuệ nhân tạo và vận hành dịch vụ, họ phải sở hữu năng lực tính toán được bảo đảm chủ quyền. Khuyến nghị này sau đó liên tục xuất hiện lặp đi lặp lại trong các văn bản chính sách của Ủy ban Châu Âu. Nhận thức rằng chỉ riêng việc đặt máy chủ ở Châu Âu là chưa đủ, mà còn phải xem xét quốc tịch và cấu trúc kiểm soát của doanh nghiệp quản lý máy chủ đó, chính là điểm khởi đầu cho đề xuất CADA.

Ủy ban Châu Âu đang thúc đẩy mục tiêu mở rộng trung tâm dữ liệu này gắn liền với một dự án riêng mang tên Nhà máy Gigafactory AI. Nhà máy Gigafactory AI là tên gọi chỉ các cơ sở tính toán siêu lớn được trang bị các cụm bộ xử lý đồ họa (GPU) quy mô lớn, một khái niệm được đưa ra trong Kế hoạch hành động Lục địa AI. Bối cảnh của dự án này là mục tiêu không dừng lại ở việc tăng số lượng máy chủ, mà là đảm bảo năng lực tính toán đủ để huấn luyện các mô hình trí tuệ nhân tạo cỡ lớn từ đầu đến cuối ngay tại Châu Âu. Cho đến nay, các nhà nghiên cứu và doanh nghiệp Châu Âu muốn huấn luyện các mô hình lớn đều phải thuê tài nguyên tính toán do các công ty đám mây của Mỹ cung cấp.

CADA và Nhà máy Gigafactory AI là nỗ lực nhằm thay đổi chính cấu trúc thuê mượn này.

Cũng cần lưu ý rằng một phần cơ sở hạ tầng hỗ trợ cho mục tiêu này đã đang đi vào hoạt động. Từ năm 2018, Liên minh Châu Âu đã cùng các quốc gia thành viên vận hành các siêu máy tính thông qua Doanh nghiệp chung về Máy tính Hiệu năng cao Châu Âu (EuroHPC Joint Undertaking). Dự án chuyển đổi các siêu máy tính hiện có như LUMI của Phần Lan hay MareNostrum của Tây Ban Nha thành

tài nguyên tính toán phục vụ huấn luyện AI đã được bắt đầu từ trước khi CADA được trình xướng.

Ý tưởng về CADA và Nhà máy Gigafactory AI không được thiết kế để thay thế hoàn toàn tài sản hiện có này, mà nhằm thu hút thêm vốn tư nhân và ngân sách các quốc gia thành viên để mở rộng quy mô trên nền tảng đó.

Mục tiêu bằng số liệu của CADA mà Ủy ban châu Âu công bố rất rõ ràng. Đó là tăng dung lượng trung tâm dữ liệu của Liên minh châu Âu lên gấp hơn ba lần trong vòng 5 đến 7 năm tới. Mục tiêu là dùng dung lượng gia tăng đó để đáp ứng nhu cầu của các doanh nghiệp và cơ quan hành chính công cho đến năm 2035. Mục tiêu này nằm ngay trong chính văn bản đề xuất do Ủy ban ban hành. Lý do mục tiêu được đặt ra lớn như vậy là vì khoảng cách giữa cung và cầu vốn đã đang mở rộng.

Văn bản "Chủ quyền công nghệ và hạ tầng kỹ thuật số Châu Âu" do Nghị viện Châu Âu thông qua ngày 22 tháng 1 năm 2026 dự báo rằng một phần đáng kể lượng tiêu thụ điện năng trên toàn thế giới phát sinh từ các trung tâm dữ liệu và thiết bị viễn thông, và tỷ trọng tiêu thụ điện năng của các trung tâm dữ liệu Châu Âu sẽ tăng lên đáng kể trong vài năm tới. Khi các phép tính trí tuệ nhân tạo tăng mạnh trên thực tế, tỷ trọng này sẽ còn gia tăng dốc hơn nữa. Nếu tốc độ xây dựng trung tâm dữ liệu không bắt kịp nhu cầu đó, Châu Âu sẽ khó thoát khỏi cảnh phải thuê đám mây của Mỹ hoặc Trung Quốc trong phát triển trí tuệ nhân tạo.

Vấn đề nằm ở chỗ bản thân việc xây dựng trung tâm dữ liệu diễn ra rất chậm. Mỗi khi có ý định dựng mới cơ sở lưu trữ dữ liệu dùng cho hành chính công trong các quốc gia hội viên, hàng loạt trường hợp đã được ghi nhận về việc thủ tục cấp phép phức tạp, quy định về đất đai và đánh giá tác động môi trường liên tục cản trở dự án. Báo cáo do Cục An ninh Thông tin Liên bang Đức và công ty luật quốc tế Bird & Bird cùng công bố ngày 27 tháng 4 năm 2026 chỉ ra rằng sự bất đồng bộ trong thủ tục hành chính giữa chính phủ liên bang và các bang của Đức đang gây ra sự chậm trễ ngay từ giai đoạn lập hồ sơ yêu cầu kỹ thuật thu mua. Sự chậm trễ này không phải là vấn đề của riêng nước Đức.

Việc các kế hoạch xây dựng máy chủ đám mây quy mô lớn bị thu nhỏ hoặc hủy bỏ do sự phản đối của cư dân địa phương hay sự chậm trễ trong thẩm định môi trường đã lặp đi lặp lại ở nhiều quốc gia Châu Âu. Trong khi chỉ riêng việc chọn địa điểm, kéo nguồn điện và xin cấp phép cho một trung tâm dữ liệu tại một khu vực đã mất nhiều năm, thì nhu cầu tính toán lại tăng lên với tốc độ nhanh hơn thế rất nhiều.

Đề xuất CADA lấy đổi mới thủ tục làm trụ cột cốt lõi nhằm giảm bớt sự chậm trễ này. Tờ báo chính trị Politico bản Châu Âu, trong bài đưa tin ngày 4 tháng 6 năm 2026, cho biết CADA khuyến nghị chính phủ các quốc gia thành viên chỉ định các khu đất có điều kiện địa lý và lưới điện thuận lợi làm khu vực tăng tốc trung tâm dữ liệu. Báo cáo tổng quan về gói chủ quyền công nghệ do công ty luật Bird & Bird tổng hợp cũng xác nhận mục đích của đề xuất là trong khu vực tăng tốc này, thủ tục cấp phép sẽ được hợp nhất qua cơ chế một cửa và thiết lập thời hạn xử lý tối đa. Đây là phương thức mà thay vì nhà đầu tư phải tìm đến từng cơ quan riêng lẻ, họ sẽ được điều phối toàn bộ chu kỳ sống của dự án tại một nơi duy nhất. Các thủ tục mà cơ chế một cửa này muốn hợp nhất rất đa dạng.

Ý tưởng là điều phối qua một đầu mối duy nhất các thủ tục vốn do nhiều cơ quan khác nhau quản lý riêng rẽ, như phê duyệt kết nối lưới điện, cấp phép cung cấp nước sinh hoạt và nước làm mát, thẩm định an toàn xây dựng, hay cấp phép đấu nối đường truyền viễn thông. Cho đến nay, nhà đầu tư phải thực hiện lần lượt từng thủ tục này, và nếu xảy ra chậm trễ ở một bước thì toàn bộ các thủ tục tiếp theo đều bị dồn tích lại. Theo báo cáo, trong khu vực tăng tốc này, thời hạn xử lý cấp phép cho các cơ sở xử lý dữ liệu mật sẽ bị giới hạn tối đa là 18 tháng.

Xét đến việc các trường hợp thủ tục cấp phép để xây dựng một cơ sở quy mô lớn phải mất nhiều năm không phải là hiếm, mức trần này được xem như một tín hiệu cho thấy ý định tái cấu trúc tận gốc bản thân quy trình thủ tục.

Cùng báo cáo này cũng cho biết quy trình đánh giá tác động môi trường được thiết kế theo hướng đơn giản hóa riêng cho các dự án nằm trong khu vực tăng tốc. Việc sự đơn giản hóa này thực sự ở mức miễn trừ hẳn khâu thẩm định môi trường hay chỉ dừng lại ở mức rút ngắn thời gian thẩm định sẽ là nội dung được cụ thể hóa khi bản đề xuất trải qua quá trình thẩm nghị của Nghị viện Châu Âu và Hội đồng Châu Âu. Ở giai đoạn hiện tại, còn quá sớm để đưa ra kết luận dựa trên các điều khoản đã cố định. Tuy nhiên, hướng đi thì rất rõ ràng. Nếu là dự án hạ tầng liên quan trực tiếp đến an ninh quốc gia, dự án đó sẽ được ưu tiên hơn so với các thủ tục cấp phép thông thường của chính quyền địa phương.

Quyền hạn chỉ định địa điểm làm khu vực tăng tốc được cho là trước tiên thuộc về chính phủ các quốc gia thành viên. Phương thức hoạt động là chính quyền địa phương hoặc chính phủ trung ương chọn lọc các khu đất bảo đảm dung lượng dự phòng của lưới điện, khả năng tiếp cận đường truyền viễn thông và an ninh vật lý rồi đề xuất lên Ủy ban châu Âu, sau đó Ủy ban sẽ xem xét và đưa vào danh sách cuối cùng. Quy trình này được đánh giá là mượn khung tương tự như phương thức chỉ định địa điểm nhà máy đúc chip mà Đạo luật Bán dẫn đã và đang thực thi.

Mục tiêu mở rộng này cũng gắn liền với các mục tiêu khí hậu của Liên minh châu Âu. Liên minh châu Âu đã ấn định mục tiêu đạt được trung hòa carbon vào năm 2050 thông qua Thỏa thuận Xanh Châu Âu. Trong bối cảnh mức tiêu thụ điện năng của các trung tâm dữ liệu liên tục gia tăng, để giữ vững mục tiêu này, áp lực phải vận hành một phần lớn các cơ sở mới xây dựng bằng năng lượng tái tạo là điều tất yếu. Việc CADA gắn các ưu đãi của khu vực tăng tốc với tiêu chuẩn bền vững có thể được hiểu là tín hiệu cho thấy sẽ không đánh đổi mục tiêu khí hậu để lấy tốc độ.

Ý tưởng về khu vực tăng tốc cũng đi kèm với rủi ro. Ưu đãi cho phép thông qua thủ tục nhanh chóng có thể dẫn đến lãng phí tiền thuế nếu thiếu cơ chế kiểm chứng xem dự án thụ hưởng ưu đãi đó có thực sự phù hợp với lợi ích công cộng hay không. Tại Thụy Điển, vào năm 2022, chính phủ đã cấp ưu đãi thuế cho các doanh nghiệp trung tâm dữ liệu nhằm mở rộng hạ tầng công nghệ trong nước, nhưng sau đó đã vấp phải chỉ trích rằng quy trình kiểm chứng xem các doanh nghiệp này có thực sự tuân thủ kế hoạch sử dụng năng lượng tái tạo hay không còn rất yếu kém. Trang tin Thụy Điển SecurityUser.com vào tháng 3 năm 2026 đã nhìn lại vấn đề này và đưa tin rằng các nước Bắc Âu đang thiết kế lại chính sách hạ tầng chủ quyền kỹ thuật số.

Báo cáo của Bird & Bird giải thích rằng đề xuất CADA bao gồm cơ chế an toàn yêu cầu các doanh nghiệp thụ hưởng ưu đãi tăng tốc phải chứng minh sự tuân thủ các tiêu chuẩn bền vững để không lặp lại thất bại này. Đơn giản hóa thủ tục vì tốc độ, nhưng đổi lại là việc đặt thêm nghĩa vụ mới về kiểm chứng kết quả.

Quy mô tài chính cho thấy thực tế CADA không phải là một đạo luật hoạt động độc lập. Văn bản kèm theo (COM(2026) 555 final/2) do Ủy ban công bố ngày 3 tháng 6 năm 2026 ước tính rằng cần tổng cộng khoản đầu tư lên tới 300 tỷ euro cho đến năm 2036 để thực thi hoàn toàn Đạo luật Phát triển Đám mây và AI cùng Gói An ninh Thế hệ mới. Trong số này, 200 tỷ euro được phân bổ cho việc mở rộng hạ tầng trung tâm dữ liệu. Văn bản này dự báo 100 tỷ euro còn lại sẽ được phân bổ thêm cho việc xây dựng nhà máy đúc chip bán dẫn và các đại công xưởng AI.

Kế hoạch đầu tư này không chỉ dành riêng cho Đạo luật Phát triển Đám mây và AI. Nếu Đạo luật Bán dẫn Châu Âu có hiệu lực năm 2023 để cập đến việc mở rộng năng lực sản xuất bán dẫn, thì kế hoạch tài chính của CADA giống như một dự án nối tiếp nhằm xử lý hạ tầng trung tâm dữ liệu và trí tuệ nhân tạo sẽ vận hành trên nền tảng bán dẫn đó. Báo cáo phân tích ngành innobu giải thích rằng hai đạo luật này kết hợp với nhau tạo thành gói chủ quyền công nghệ của Châu Âu. Con số này hoàn toàn là ước tính của Ủy ban, còn ngân sách thực hiện thực tế chỉ được xác

định sau khi trải qua các cuộc đàm phán ngân sách giữa các quốc gia thành viên và Nghị viện Châu Âu.

Việc các lãnh đạo Liên minh châu Âu họp tại Berlin vào ngày 18 tháng 11 năm 2025 và ra Tuyên bố chung Hội nghị thượng đỉnh An ninh được nhắc đến như bối cảnh chính trị của kế hoạch tài chính này.

Bản chất của mối đe dọa mà sự mở rộng hạ tầng này hướng đến giải quyết mang tính chất khác hẳn so với việc chặn truy cập mô hình đã xem xét ở Chương 2. Vụ việc Anthropic tạm dừng quyền truy cập của người nước ngoài đối với Fable 5 là chuyện diễn ra ở tầng phần mềm. Chỉ với một lệnh kiểm soát xuất khẩu từ chính phủ Mỹ, bản thân quyền truy cập vào một mô hình cụ thể đã bị chặn đứng. Ngược lại, mối đe dọa phát sinh khi không sở hữu trung tâm dữ liệu lại mang tính căn bản hơn. Nếu ở trong thế phải đi thuê chính năng lực tính toán từ các doanh nghiệp nước ngoài, điều đó có nghĩa là không chỉ mô hình, mà ngay cả quyền truy cập vào phần cứng chạy mô hình đó cũng có thể bị khóa lại. Điều mà CADA nhắm tới chính là điểm yếu ở tầng phần cứng này.

Tổng hợp đưa tin từ hãng luật Bird & Bird và tạp chí công nghệ ITWelt, đề xuất CADA được cho là đã đưa ra chỉ tiêu thúc đẩy một phần lớn doanh nghiệp tư nhân trong khu vực châu Âu chuyển sang dịch vụ đám mây chủ quyền cho đến năm 2030. Đồng thời, kế hoạch bố trí dày đặc các căn cứ tính toán biên độ trễ thấp trên khắp châu lục nhằm giảm sự phụ thuộc vào các nền tảng lớn của Mỹ ngay trong lĩnh vực dịch vụ tiêu dùng cũng được đề cập. Việc liệt kê các mục tiêu này có được giữ lại làm nghĩa vụ bắt buộc hay hạ xuống mức khuyến nghị trong quy định cuối cùng vẫn cần phải theo dõi qua quá trình xem xét.

Việc chỉ định ưu tiên này đi kèm với cái giá phải trả là tiếng nói của cộng đồng địa phương bị thu hẹp. Khi trung tâm dữ liệu được xếp vào dạng dự án chiến lược quan trọng cấp quốc gia, phạm vi mà cư dân tại khu đất đó có thể đưa ra phản đối hoặc tham gia điều thanh công khai trong quy trình quy hoạch đô thị thông thường có thể bị hạn chế. Cắt giảm thủ tục để đổi lấy tốc độ cũng đồng nghĩa với việc làm giảm bớt tiếng nói của người dân địa phương vốn được lồng ghép trong các thủ tục đó. Việc CADA sẽ cân bằng yếu tố này như thế nào trong văn bản cuối cùng vẫn chưa được ấn định.

Về phương thức bảo đảm nguồn điện, cách tiếp cận giữa các nước thành viên cũng có sự phân hóa. Pháp, quốc gia có tỷ trọng điện hạt nhân cao, đang quyết liệt thúc đẩy chính sách xây dựng trung tâm dữ liệu ở khu vực lân cận các nhà máy điện hạt nhân. Khả năng cung cấp trực tiếp nguồn điện carbon thấp ổn định cho trung tâm dữ liệu được coi là ưu điểm của cách làm này. Trái lại, các quốc gia tái cơ cấu

lưới điện xoay quanh năng lượng tái tạo phải tự tìm lời giải riêng cho việc làm sao phối hợp tính chập chờn của điện mặt trời và điện gió với nhu cầu hoạt động 24/7 của trung tâm dữ liệu. Việc đưa điều kiện lưới điện vào tiêu chí xác định khu vực gia tốc của CADA cho thấy đây dường như là thiết kế đã tính đến sự khác biệt về hoàn cảnh của từng nước.

Khả năng việc chỉ định khu vực gia tốc bị tập trung vào một số nước thành viên nhất định cũng đang được đem ra thảo luận. Nhiều khả năng một số khu vực ở Tây Âu và Bắc Âu, vốn đã có lưới điện và hạ tầng viễn thông hoàn thiện, sẽ đáp ứng điều kiện chỉ định trước; trong khi một số khu vực tại Đông Âu và Nam Âu với tiến độ đầu tư hạ tầng tương đối chậm lại có nguy cơ bị tụt lại phía sau. Làm sao để dung hòa giữa nguyên tắc phát triển cân bằng vùng của Liên minh châu Âu và logic tốc độ của việc gia tốc trung tâm dữ liệu vẫn là bài toán cần giải quyết trong quá trình CADA hoàn thiện các điều khoản cuối cùng.

Bức tranh mà CADA phác thảo rất cuộc quy về một câu hỏi duy nhất. Nếu châu Âu không thể tự mình xây dựng không gian vật lý để lưu trữ dữ liệu của chính mình, việc bàn về chủ quyền của phần mềm vận hành trên nền tảng đó cũng trở thành điều rỗng tuếch. Trên nền móng các trung tâm dữ liệu vật lý còn tồn tại một tầng nữa. Đó chính là tiêu chí phân định ai là người kiểm soát trung tâm dữ liệu đó.

---

## **Căn cứ và tài liệu tham khảo**

1. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
2. European Commission, 'Cloud computing', 2026, <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing>
3. Cecilia Rikap, 'Does Europe Really Have a Plan for Tech Sovereignty?', TechPolicy.Press, ngày 15 tháng 6 năm 2026, <https://www.techpolicy.press/does-europe-really-have-a-plan-for-tech-sovereignty-cada/>
4. Mario Draghi, 「The Future of European Competitiveness」, European Commission, tháng 9 năm 2024.
5. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', Công báo Nghị viện Châu Âu, ngày 22 tháng 1 năm 2026.
6. Cơ quan An ninh Thông tin Liên bang Đức, 「Digitale Souveränität bei IT-Vergaben: Zwischen politischem Anspruch und vergaberechtlicher Wirklichkeit」, Bird & Bird Insights, ngày 27 tháng 4 năm 2026.
7. Tyler Weygold, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, ngày 4 tháng 6 năm 2026, <https://www.politico.eu/video/achieving-digital-sovereignty-a-golden-opportunity-for-the-eu-politico/>
8. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, ngày 23 tháng 6 năm 2026.

9. SecurityUser.com, 'Ny molnpolicy ska ge ökad digital suveränitet i offentlig förvaltning', SecurityUser.com, tháng 3 năm 2026.
10. European Commission, COM(2026) 555 final/2, Công báo Liên minh Châu Âu, ngày 3 tháng 6 năm 2026.
11. innobu, 'EU Tech Sovereignty 2026: Chips Act 2.0 and CAIDA', innobu Insights, tháng 6 năm 2026.
12. Ban biên tập Itwelt, 'Best European cloud alternatives: Top 10 of 2026', Itwelt, tháng 2 năm 2026.

## 4.2 Thiết kế 4 cấp độ bảo đảm chủ quyền (Sovereignty Assurance Levels) của CADA

Trục thứ hai do đề xuất CADA thiết lập không phải là vỏ bọc vật lý mang tên trung tâm dữ liệu, mà là tiêu chuẩn để xác định quốc tịch của phần mềm chạy bên trong và doanh nghiệp vận hành phần mềm đó. Ủy ban Châu Âu đã chia tiêu chuẩn này thành bốn cấp độ. Bằng tiếng Anh, nó được gọi là Cấp độ Bảo đảm Chủ quyền (Sovereignty Assurance Level), gọi tắt là SEAL. Báo cáo do Viện Nghiên cứu An ninh Thông tin Bloomsbury (BISI), một cơ quan nghiên cứu chính sách an ninh tại Luân Đôn, công bố ngày 7 tháng 7 năm 2026 đã xếp cấu trúc bốn cấp độ này là một trong ba trục của CADA, đồng thời giải thích rằng mục đích thiết kế của nó là nhằm ngăn chặn ảnh hưởng của Đạo luật CLOUD (CLOUD Act) và Điều 702 Đạo luật Giám sát Tình báo Nước ngoài của Mỹ đối với dữ liệu công của Châu Âu.

Đạo luật CLOUD được Quốc hội Mỹ thông qua vào năm 2018 buộc các nhà cung cấp dịch vụ công nghệ thông tin và truyền thông do pháp nhân Mỹ chi phối quản lý phải có nghĩa vụ bảo lưu và cung cấp dữ liệu cho cơ quan điều tra, bất kể dữ liệu đó được lưu trữ ở quốc gia nào. Điều khoản này, được xác nhận trong văn bản đạo luật và bản tóm tắt của Quốc hội, cũng có thể áp dụng cho các công ty con của doanh nghiệp Mỹ được thành lập tại Châu Âu. Điều này có nghĩa là ngay cả khi ký hợp đồng với doanh nghiệp Châu Âu, đặt máy chủ trong lãnh thổ Châu Âu và tuân thủ luật bảo vệ dữ liệu cá nhân của Châu Âu, nếu công ty mẹ của công ty vận hành máy chủ đó là một pháp nhân Mỹ thì yêu cầu của cơ quan điều tra Mỹ vẫn có thể được ưu tiên hơn hợp đồng.

Tài liệu làm việc kèm theo (SWD(2026) 502 final) do Ủy ban Châu Âu ban hành cùng với đề xuất CADA được cho là đã phân tích chi tiết vấn đề thẩm quyền tài phán ngoài lãnh thổ này.

Không nên nhầm lẫn hệ thống SEAL với luật bảo vệ dữ liệu cá nhân. Quy định Chung về Bảo vệ Dữ liệu (GDPR) của Liên minh Châu Âu là đạo luật quy định cách thức thu thập và xử lý dữ liệu cá nhân, vốn đã có hiệu lực từ năm 2018. Việc tuân thủ GDPR không giải quyết được vấn đề quốc tịch của công ty xử lý thông tin đó. Dù thông tin có được mã hóa an toàn đến đâu và chỉ thu thập đúng mức cần thiết, nếu công ty lưu trữ thông tin đó là một pháp nhân Mỹ thì sự bảo vệ của GDPR vẫn bộc lộ giới hạn trước các yêu cầu pháp lý từ chính phủ Mỹ. Điều GDPR quy định là cách thức xử lý thông tin, còn điều SEAL muốn quy định là quốc tịch và cơ cấu chi phối của công ty xử lý thông tin đó.

Hai đạo luật nhìn nhận cùng một dữ liệu ở các tầng nấc khác nhau.

Tòa án Châu Âu đã từng trực tiếp đối mặt với vấn đề này. Vào tháng 7 năm 2020, trong phán quyết thường gọi là Schrems II, Tòa án Công lý Châu Âu đã tuyên bố thỏa thuận chuyển giao dữ liệu cá nhân giữa Liên minh Châu Âu và Mỹ mang tên Lá chắn Quyền riêng tư (Privacy Shield) là vô hiệu, với lý do pháp luật giám sát của Mỹ cho phép các cơ quan tình báo Mỹ tiếp cận dữ liệu truyền thông. Nội dung cốt lõi của phán quyết này là dù có đưa các điều khoản bảo vệ dữ liệu cá nhân chặt chẽ đến đâu vào hợp đồng, chừng nào đối tác hợp đồng vẫn chịu sự điều chỉnh của pháp luật Mỹ thì bản thân khả năng tiếp cận của các cơ quan tình báo Mỹ cũng không thể bị ngăn chặn bằng hợp đồng.

Tích lũy từ những trải nghiệm tư pháp như vậy chính là bối cảnh khiến CADA quyết định phân chia cấp độ chủ quyền dựa trên tiêu chuẩn gốc rễ hơn nhiều so với các điều khoản hợp đồng: đó là quốc tịch và cơ cấu chi phối. Bài học an ninh mà Châu Âu rút ra được rất cuộc là: cơ cấu chi phối và quốc tịch của công ty mới là tấm lá chắn thực sự, chứ không phải các điều khoản trên văn bản hợp đồng.

Bài học này cũng dẫn đến những phản ứng trên thị trường. Trong những năm gần đây, Amazon, Microsoft và Google đã đưa ra các sản phẩm đám mây chủ quyền mang tên gọi riêng của mình nhằm vào khách hàng Châu Âu. Lời hứa lưu trữ và xử lý dữ liệu hoàn toàn trong nội bộ Châu Âu, đồng thời hạn chế sự tiếp cận của nhân viên không phải người Châu Âu là khẩu hiệu quảng cáo chung của các sản phẩm này. Tuy nhiên, hiếm khi các sản phẩm này chuyển giao cả cổ phần chi phối và quyền biểu quyết của hội đồng quản trị sang cho Châu Âu như yêu cầu của Cấp 3 và Cấp 4 — các cấp độ cao hơn của SEAL. Việc Châu Âu hóa vị trí máy chủ cùng quy định vận hành và việc Châu Âu hóa bản thân quyền sở hữu công ty là những lời hứa ở hai cấp độ hoàn toàn khác nhau.

Điều mà hệ thống SEAL muốn làm chính là phân biệt hai cấp độ này và ghi rõ trong tiêu chuẩn mua sắm công.

Về một ví dụ cụ thể, Amazon Web Services vào năm 2023 đã công bố dự án đám mây chủ quyền Châu Âu bằng cách thành lập một pháp nhân riêng cho Châu Âu với hội đồng quản trị và ban điều hành gồm các công dân Châu Âu. Đó là lời hứa đặt dữ liệu lưu trữ và nhân sự vận hành tại Châu Âu. Thế nhưng, cổ phần cuối cùng của pháp nhân Châu Âu này vẫn do công ty mẹ ở Mỹ là Amazon.com nắm giữ. Điều mà Cấp 3 và Cấp 4 của SEAL yêu cầu chính là việc chuyển đổi cả cơ cấu cổ phần cuối cùng này sang sở hữu của Châu Âu, nên các sản phẩm đám mây chủ quyền theo mô hình này dù có thể đạt điều kiện ở các cấp độ thấp hơn thì cũng khó lòng vượt qua ngưỡng cửa của các cấp độ cao hơn.

Cấp 1 của SEAL yêu cầu những điều kiện cơ bản nhất. Đó là việc lưu trữ và xử lý dữ liệu phải được thực hiện tại các cơ sở nằm trong lãnh thổ Liên minh Châu Âu. Cấp độ này áp dụng cho các công việc hành chính thông thường có độ bảo mật quốc gia thấp; chi nhánh tại Châu Âu của các doanh nghiệp ngoài khu vực, bao gồm cả doanh nghiệp Mỹ, nếu có trung tâm dữ liệu tại Châu Âu thì đều đáp ứng tiêu chuẩn này và có thể tham gia đấu thầu. Việc phê duyệt được thực hiện theo hình thức tự xác nhận, trong đó nhà cung cấp tự tuyên bố đáp ứng điều kiện, và không yêu cầu kiểm toán bên thứ ba riêng biệt.

Cấp 2 vượt qua khía cạnh dữ liệu nằm ở đâu về mặt vật lý để xem xét đến cả chuỗi cung ứng phần mềm xử lý dữ liệu đó. Nhà cung cấp phải nộp Danh mục Thành phần Phần mềm (SBOM) ghi chép chi tiết các thành phần phần mềm, đồng thời phải trải qua kiểm minh lỗ hổng bảo mật của mã nguồn. Danh mục Thành phần Phần mềm là danh sách ghi rõ từng chi tiết xem một chương trình được cấu thành từ những linh kiện nào, tức là các thư viện bên ngoài và thành phần mã nguồn mở nào. Có thể dễ dàng hiểu đây là khái niệm tương tự như nhãn ghi thành phần nguyên liệu trên thực phẩm.

Mục đích là khi phát hiện lỗi bảo mật ở một thành phần nào đó, người dùng có thể nhanh chóng đối chiếu danh sách để xem lỗi đó có tồn tại trong hệ thống mình đang sử dụng hay không. Theo báo cáo của BISI, cấp độ này được thiết kế để áp dụng cho các dịch vụ công có độ nhạy cảm ở mức trung bình như thông tin y tế hay hạ tầng tài chính. Ngay cả doanh nghiệp ngoài khu vực, nếu liên doanh với doanh nghiệp Châu Âu để chia sẻ cơ cấu chi phối và chứng minh được cơ chế cách ly kỹ thuật, thì vẫn có con đường mở ra để đạt được tư cách ở cấp độ này.

Từ Cấp 3 trở đi, các yêu cầu trở nên nghiêm ngặt một cách rõ rệt. Trụ sở chính của doanh nghiệp cung cấp dịch vụ xử lý dữ liệu và các doanh nghiệp nhà thầu phụ của doanh nghiệp đó phải thực sự nằm trong lãnh thổ Liên minh Châu Âu, đồng thời cổ phần chi phối và quyền biểu quyết của hội đồng quản trị phải nằm trong tay công dân mang quốc tịch Liên minh Châu Âu. Nhân sự nòng cốt bảo trì hệ thống cũng phải là cư dân mang quốc tịch Liên minh Châu Âu và phải vượt qua vòng thẩm tra lý lịch. Tuy nhiên, báo cáo của BISI cho biết Ủy ban Châu Âu đã để lại một lối đi ngoại lệ trong bản đề xuất, theo đó nói lỏng một phần yêu cầu này đối với các quốc gia đồng minh đã ký hiệp định chia sẻ thông tin với Liên minh Châu Âu và không có xung đột tư pháp. Cấp độ này áp dụng cho các nhiệm vụ liên quan trực tiếp đến an ninh như mạng lưới điều tra trật tự trị an quốc gia hay phân tích mối đe dọa khủng bố.

Việc ngoại lệ dành cho quốc gia đồng minh trên thực tế sẽ được áp dụng cho những nước nào vẫn chưa được xác định. Những quốc gia đã có sẵn hiệp định chia sẻ thông tin và thể chế hợp tác tư pháp với Liên minh Châu Âu được đưa ra làm ứng viên, nhưng danh sách quốc gia cụ thể chưa được công khai ở giai đoạn đề xuất. Sự mơ hồ này được coi là một trong những điểm sẽ trở thành đối tượng đàm phán gay gắt nhất trong quá trình CADA được thẩm định. Nếu quy định phạm vi ngoại lệ quá rộng thì tính hiệu lực của Cấp 3 sẽ bị mờ nhạt, còn nếu quy định quá hẹp thì phải chấp nhận ma sát ngoại giao với các nước đồng minh.

Nếu khó hình dung cả bốn cấp độ cùng lúc, có thể liên tưởng đến hệ thống kiểm soát ra vào ㄹ một tòa nhà. Ở sảnh lớn, bất kỳ ai có thẻ khách cũng có thể bước vào; lên tầng văn phòng phải có thẻ nhân viên; phòng máy chủ chỉ dành cho số ít người có phê duyệt riêng; còn phòng kết sắt ở trong cùng chỉ cực kỳ ít người đã qua kiểm tra lý lịch mới được phép truy cập. Bốn cấp độ của SEAL cũng tương tự: trọng lượng của thông tin xử lý càng lớn thì phạm vi chủ thẻ được cấp quyền truy cập càng thu hẹp.

Cấp độ 4 là cấp độ không có ngoại lệ. Cấp độ này áp dụng cho các lĩnh vực liên quan trực tiếp đến sự tồn vong của quốc gia như quốc phòng, bí mật quân sự hay phân tích an ninh cấp cao nhất, vừa tuân thủ nghiêm ngặt các yêu cầu về quốc tịch của hội đồng quản trị và nhân sự ở Cấp độ 3, vừa không chấp nhận bất kỳ ngoại lệ nào ngay cả đối với các quốc gia đồng minh. Từ khâu thiết kế hệ thống cho đến bảo trì mã nguồn, mọi khả năng can thiệp của vốn thương mại nước ngoài đều bị loại bỏ hoàn toàn từ gốc. Nhà cung cấp phải đạt cấp độ High (Cao) – mức cao nhất trong Khung Chứng nhận An ninh Mạng Châu Âu (EUCS) do Cơ quan An ninh Mạng Liên minh Châu Âu (ENISA) cấp – mới được tham gia đấu thầu. Khung chứng nhận EUCS này không phải do CADA tạo ra đầu tiên.

ENISA đã chuẩn bị khung chứng nhận này từ nhiều năm trước, và giữa các quốc gia thành viên được cho là đã tồn tại những bất đồng kéo dài xung quanh việc có nên đưa điều khoản hạn chế sở hữu cổ phần của các công ty phi Châu Âu vào cấp độ cao nhất hay không. Một số quốc gia thành viên, đứng đầu là Pháp, đã kiên quyết yêu cầu hạn chế tỷ lệ sở hữu, trong khi các quốc gia khác phản đối với lý do rào cản này gây hại cho cạnh tranh thị trường. Việc CADA viện dẫn rõ ràng cấp độ High của EUCS vào các yêu cầu của Cấp độ 4 được xem là một nỗ lực nhằm gia tăng sức nặng pháp lý cho cuộc tranh luận về quyền sở hữu vốn chưa thể đi đến kết luận trong khung chứng nhận trước đó.

Báo cáo của BISI cũng đưa ra ước tính về tỷ lệ áp dụng bốn cấp độ này trong hoạt động mua sắm công thực tế. Trong tổng số các dự án ứng dụng công nghệ trong

khu vực công, các nghiệp vụ hành chính thông thường có độ nhạy cảm thấp chiếm khoảng 70% và được xếp vào Cấp độ 1. Các nghiệp vụ có độ nhạy cảm trung bình, chiếm khoảng 20%, được xếp vào Cấp độ 2. 10% còn lại được chia cho Cấp độ 3 và Cấp độ 4, trong đó báo cáo dự báo 9% sẽ thuộc Cấp độ 3 và 1% thuộc Cấp độ 4. Cần làm rõ rằng con số ước tính này chưa phải là thống kê chính thức mà chỉ là dự báo dựa trên phân tích của báo cáo. Dù vậy, ý nghĩa mà tỷ lệ này gợi mở là rất rõ ràng.

Đó là đại đa số các thương vụ mua sắm công vẫn nằm ở Cấp độ 1 và Cấp độ 2, còn Cấp độ 3 và Cấp độ 4 – những cấp độ yêu cầu quyền sở hữu hoàn toàn thuộc về Châu Âu – chỉ áp dụng cho một phần cực kỳ nhỏ trong tổng số các dự án.

Thiết kế theo từng cấp độ này không phải là một phát minh hoàn toàn mới. Pháp đã vận hành khung chứng nhận riêng mang tên SecNumCloud, đồng thời yêu cầu chứng nhận cấp cao nhất đối với các trường hợp sử dụng an ninh cấp cao của quốc gia nhằm chặn đứng từ gốc ảnh hưởng của Đạo luật CLOUD Hoa Kỳ. Chứng nhận này do Cơ quan An ninh Hệ thống Thông tin Quốc gia Pháp (ANSSI) quản lý, và các nhà cung cấp dịch vụ đám mây muốn đạt cấp độ cao nhất bắt buộc phải có vốn của Pháp hoặc Liên minh Châu Âu nắm giữ cổ phần chi phối. Báo cáo của BISI đánh giá rằng cấu trúc 4 cấp độ của CADA là một thiết kế mở rộng logic của khung chứng nhận kiểu Pháp này lên quy mô toàn Liên minh Châu Âu.

Nhờ đã có cơ chế được thực thi tại Pháp từ trước, nên lập luận cho rằng CADA không phải là một cuộc thử nghiệm hoàn toàn mới mà là đề xuất mở rộng một mô hình đã qua kiểm chứng trở nên hoàn toàn có căn cứ.

Bên cạnh SecNumCloud của Pháp, một số quốc gia thành viên khác cũng phát triển các khung chứng nhận độc lập theo cách riêng của mình. Nếu tiêu chuẩn giữa các nước khác nhau, sự kém hiệu quả sẽ xuất hiện khi một nhà cung cấp đã được chứng nhận tại một quốc gia lại phải trải qua quy trình thẩm định lại từ đầu khi tham gia mua sắm công ở quốc gia khác. Đây chính là lý do CADA muốn hợp nhất các tiêu chuẩn này thành một hệ thống SEAL duy nhất. Nếu 27 quốc gia thành viên cứ khăng khăng giữ các tiêu chuẩn chứng nhận riêng biệt, một thị trường đám mây chủ quyền bao phủ toàn Châu Âu khó có thể hình thành ngay từ đầu.

Quy trình phê duyệt cũng có mức độ nghiêm ngặt khác nhau tùy theo từng cấp độ. Cấp độ 1 chỉ cần sự tự cam kết của nhà cung cấp là được thông qua, đồng thời một luồng xử lý rút gọn được thiết lập cho các doanh nghiệp vừa và nhỏ nhằm miễn trừ việc thẩm định hồ sơ hai lần. Trái lại, từ Cấp độ 2 đến Cấp độ 4, một tổ chức kiểm toán độc lập bên thứ ba do Liên minh Châu Âu chỉ định phải thẩm định

tỉ mỉ ngay từ sơ đồ thiết kế gốc của hệ thống, sau đó cơ quan chuyên trách của quốc gia thành viên mới đưa ra phê duyệt cuối cùng. Quyết định phê duyệt do một quốc gia thành viên đưa ra sẽ được đăng tải lên sổ đăng ký chung của Liên minh Châu Âu và trải qua thời hạn thẩm tra lẫn nhau kéo dài 60 ngày để các nước thành viên khác có thể đưa ra phản đối. Nếu các bất đồng không được giải quyết trong thời gian này, quy trình đề xuất Ủy ban Châu Âu đưa ra phương án điều chỉnh cuối cùng để khép lại tranh chấp.

Việc cho phép tất cả 27 quốc gia thành viên xem xét lại quyết định của một nước dường như là một thiết kế nhằm ngăn ngừa kẻ hở, tránh trường hợp sự thẩm định lỏng lẻo của một quốc gia làm hạ thấp tiêu chuẩn an ninh của toàn bộ Liên minh.

Chúng nhận không phải là thứ nhận một lần là xong. Nếu cơ cấu sở hữu cổ phần 또는 thành phần hội đồng quản trị của nhà cung cấp thay đổi, bản thân tiền đề của cấp độ SEAL từng đạt được ban đầu có thể bị sụp đổ. Vẫn còn đó câu hỏi: nếu một công ty từng đạt chứng nhận doanh nghiệp Châu Âu sau này bị thôn tóm bởi vốn phi Châu Âu, tư cách thực hiện các hợp đồng công của công ty đó sẽ ra sao? Báo cáo của BISI cho biết CADA có bao gồm cả các quy trình giám sát và tái thẩm định những thay đổi sau chứng nhận này, tuy nhiên tần suất và mức độ nhanh chóng của việc tái thẩm định vẫn chưa được cụ thể hóa.

Câu hỏi về việc ai là người quyết định các cấp độ này cũng vẫn còn đó. Trước khi đưa một dự án mới ra đấu thầu mua sắm công, cơ quan nhà nước phải tự đánh giá độ nhạy cảm của dữ liệu mà dự án đó xử lý để xác định dự án tương ứng với cấp độ SEAL nào. Một dự án xử lý các tài liệu hành chính thông thường sẽ xếp vào Cấp độ 1, nhưng ngay tại cùng cơ quan đó, nếu dự án làm việc với thông tin an ninh 또는 quốc phòng thì có thể bị xếp vào Cấp độ 3 또는 Cấp độ 4. Nếu đánh giá này bị sai, rắc rối sẽ bộc lộ muộn về sau. Trường hợp hợp đồng được ký kết dưới một cấp độ thấp nhưng sau đó dữ liệu mới được xác nhận là liên quan trực tiếp đến an ninh quốc gia, bên mua sẽ rơi vào thế buộc phải chỉnh sửa lại hợp đồng đã ký.

Có thể hiểu rằng việc đề xuất của CADA quy định đồng thời cả quy trình xác định lẫn hệ thống kiểm toán là nhằm giảm thiểu nguy cơ phân loại sai này.

Gánh nặng chứng nhận không phải lúc nào cũng nhẹ nhàng đối với riêng các doanh nghiệp lớn. Việc lập danh mục nguyên vật liệu phần mềm và thẩm định mã nguồn - vốn được yêu cầu từ Cấp độ 2 trở đi - đòi hỏi nhân lực chuyên trách cùng chi phí không nhỏ. Đối với các doanh nghiệp đám mây mới khởi nghiệp tại Châu Âu có tiềm lực tài chính hạn chế, rào cản này có thể ngăn cản ngay chính khả năng gia nhập thị trường của họ. Cho dù CADA có mở luồng thủ tục đơn giản hóa

ở Cấp độ 1 cho các doanh nghiệp vừa và nhỏ, nếu không có các biện pháp hỗ trợ kèm theo để giúp các doanh nghiệp Châu Âu đang trong giai đoạn phát triển vươn lên các cấp độ cao hơn, một nghịch lý sẽ xuất hiện: thị trường ở các cấp độ cao hơn rốt cuộc lại chỉ mở ra cho số ít đại công ty đã có sẵn tiềm lực tài chính.

Để cấu trúc bốn cấp độ này thực sự đi vào vận hành, vẫn còn những ngọn núi phải vượt qua. Nhiều báo cáo trong ngành cũng chỉ ra rằng thị trường Châu Âu hiện chưa có đủ năng lực cung ứng từ các doanh nghiệp nội địa để đáp ứng được các yêu cầu ở Cấp độ 3 và Cấp độ 4. Lý do các doanh nghiệp Châu Âu cần có thời gian mới đáp ứng được các điều kiện ở các cấp độ cao hơn không chỉ dừng lại ở bài toán ý chí chính trị. Để vận hành các dịch vụ đám mây quy mô lớn, doanh nghiệp cần khoản đầu tư ban đầu khổng lồ vào phần cứng máy chủ, hạ tầng mạng và thiết bị làm mát; đồng thời để thu hồi khoản đầu tư đó, họ phải xây dựng được tập khách hàng ổn định qua một khoảng thời gian dài.

Các công ty điện toán đám mây lớn của Mỹ đã mất hàng thập kỷ để xây dựng nên vòng tuần hoàn đầu tư và thu hồi vốn này. Có ý kiến chỉ ra rằng, để các doanh nghiệp châu Âu bắt kịp vòng tuần hoàn này trong một khoảng thời gian ngắn, chỉ riêng các tiêu chuẩn phân hạng do CADA quy định là chưa đủ, mà cần phải đi kèm với sự hỗ trợ vốn riêng biệt dành cho các doanh nghiệp đáp ứng những cấp độ đó. Dù các yêu cầu có được thiết kế tinh vi đến đâu, nếu thiếu các doanh nghiệp vượt qua được những yêu cầu đó, các cơ quan công quyền cuối cùng cũng sẽ phải lùi bước về mức thu mua cấp thấp hơn hoặc phụ thuộc vào các điều khoản ngoại lệ. So với bản thân các cấp độ do CADA quy định, tốc độ phát triển năng lực của các doanh nghiệp châu Âu nhằm đáp ứng các cấp độ đó mới chính là biến số quyết định sự thành bại thực tế của cơ chế này.

---

## **Căn cứ và tài liệu tham khảo**

1. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), ngày 7 tháng 7 năm 2026.
2. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018, <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>
3. European Commission, SWD(2026) 502 final, Công báo Liên minh châu Âu, ngày 3 tháng 6 năm 2026, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502>
4. European Commission, 'Cloud and AI Development Act', Shaping Europe's digital future, Công báo Liên minh châu Âu, ngày 3 tháng 6 năm 2026.
5. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, ngày 23 tháng 6 năm 2026.
6. Court of Justice of the European Union, Judgment in Case C-311/18 (Data Protection Commissioner v Facebook Ireland and Maximilian Schrems), ngày 16 tháng 7 năm 2020.

### 4.3 'Quyền chấm dứt hợp đồng vì lý do chủ quyền (Sovereignty Termination Clause)' và việc thể chế hóa nghĩa vụ về tính khả di

Dù CADA có thiết kế hệ thống phân cấp tinh vi đến đâu, nếu không trả lời được câu hỏi làm thế nào để chấm dứt các hợp đồng đã ký kết, thì hệ thống phân cấp đó cũng chỉ là một chế độ nửa vời, áp dụng cho những dự án mới bắt đầu. Trường hợp của Vương quốc Anh thể hiện rõ nhất vấn đề này.

Cơ quan Y tế Quốc gia Anh (NHS) năm 2023 đã ký hợp đồng trị giá 330 triệu bảng Anh với Palantir để xây dựng Nền tảng Dữ liệu Hợp nhất (Federated Data Platform). Nền tảng này là một hệ thống gom thông tin bệnh nhân, tình trạng giường bệnh và danh sách chờ của các bệnh viện trên khắp nước Anh vào một hệ thống chung để phân tích. Ủy ban Khoa học và Công nghệ Hạ viện Anh đã phát hành một báo cáo cảnh báo rằng hợp đồng này là một lỗ hổng khó chấp nhận về mặt an ninh quốc gia. Cơ quan truyền thông thiên tả Novara Media đưa tin nhiều hạ nghị sĩ đã yêu cầu chính phủ chấm dứt hợp đồng này. Vấn đề nằm ở chỗ, ngay cả khi muốn chấm dứt hợp đồng, việc đó cũng không thể thực hiện một cách dễ dàng.

Theo báo cáo của Ủy ban Khoa học và Công nghệ Hạ viện, dù NHS đã trả phí dịch vụ trong suốt thời hạn hợp đồng, họ vẫn không nhận được tài sản cốt lõi của hệ thống là Mô hình Dữ liệu Chuẩn (Canonical Data Model) và quyền sở hữu trí tuệ đối với bộ thực thể (ontology). Thời điểm hợp đồng kết thúc, những gì còn lại trong tay NHS không phải là dữ liệu, mà là tàn tích dữ liệu được thiết kế để chỉ hoạt động trên phần mềm của Palantir. Thực tế là điều khoản quyền chấm dứt hợp đồng theo lý do trong hợp đồng này chỉ có hiệu lực vào tháng 2 năm 2027 cũng đã được xác nhận qua báo cáo của Hạ viện. Nói cách khác, có một khoảng trống kéo dài vài năm giữa thời điểm thực sự muốn chấm dứt hợp đồng và thời điểm pháp lý thực sự có thể chấm dứt.

Các hợp đồng mua sắm công vốn dĩ đã có điều khoản chấm dứt. Những điều khoản chấm dứt khi có vi phạm hợp đồng, hoặc điều khoản chấm dứt tùy ý chịu tiền phạt bồi thường mà không cần lý do đặc biệt thường được sử dụng phổ biến. Điều mà CADA muốn mới đưa vào là danh mục thứ ba, phân biệt với hai loại này. Ngay cả khi nhà cung cấp đang thực hiện hợp đồng một cách thiện chí, nếu quốc tịch và cơ cấu kiểm soát của nhà cung cấp đó bị đánh giá là mối đe dọa đối với an

ninh quốc gia, thì chính quyền vẫn có căn cứ riêng để chấm dứt hợp đồng mà không phải bồi thường tiền phạt. Nếu các lý do như vậy không được định nghĩa rõ ràng về mặt pháp lý, ngược lại, nó cũng để lại dư địa cho nhà cung cấp khởi kiện với lý do chấm dứt tùy tiện.

Vấn đề mà trường hợp này bộc lộ không chỉ giới hạn ở một công ty cụ thể là Palantir. Khi các cơ quan công bắt đầu giao dữ liệu cho một phần mềm cụ thể, dữ liệu đó dần dần bị khống chế để chỉ có ý nghĩa trong cấu trúc riêng của phần mềm đó. Việc chuyển dữ liệu sang một hệ thống khác không chỉ dừng lại ở việc sao chép tệp. Nhiều trường hợp phải thiết kế lại chính hệ thống phân loại và cấu trúc quan hệ chứa dữ liệu, tức là bộ thực thể (ontology). Bộ thực thể có thể coi là bản thiết kế định nghĩa những thông tin nào có mối quan hệ ra sao với nhau. Chẳng hạn, hệ thống quy tắc quy định cách kết nối giữa bệnh nhân, giường bệnh và hồ sơ khám chữa bệnh chính là thuộc về khái niệm này.

Công việc tái thiết lập hệ thống quy tắc này cho phù hợp với hệ thống của một công ty khác đòi hỏi hợp đồng mới, nhân lực phát triển và ngân sách đáng kể. Nghịch lý xuất hiện ở đây khi việc mua sắm vốn trông có vẻ rẻ ở giai đoạn đầu hợp đồng lại đòi hỏi chi phí lớn hơn cả hợp đồng ban đầu tại thời điểm chuyển đổi. Hiệu ứng khóa cấu trúc này thường được giới công nghiệp gọi là sự phụ thuộc nhà cung cấp (vendor lock-in).

Hiệu ứng khóa mà trường hợp NHS cho thấy không chỉ giới hạn ở các cơ sở dữ liệu truyền thống. Trong việc mua sắm ở thời đại trí tuệ nhân tạo, đối tượng chuyển giao không chỉ bao gồm dữ liệu mà còn cả mô hình được huấn luyện bằng dữ liệu đó, các giá trị cấu hình đã tinh chỉnh mô hình, và cả nhúng (embedding) được dùng trong tìm kiếm. Nếu nhà cung cấp lưu trữ các yếu tố này dưới định dạng độc quyền, thì sau khi hợp đồng kết thúc, những gì còn lại cho cơ quan công chỉ là hạ tầng trống rỗng, còn trí tuệ tích lũy trên đó vẫn hoàn toàn nằm trong tay nhà cung cấp. Có ý kiến cho rằng để nghĩa vụ về tính khả di của CADA mang lại hiệu quả thực tế, cần có các quy định chi tiết đưa cả những tài sản đặc thù của trí tuệ nhân tạo này vào đối tượng chuyển giao.

Phương pháp phổ biến nhất để bảo đảm tính khả di về mặt kỹ thuật là bắt buộc sử dụng các tiêu chuẩn mở. Nếu quy định rõ trong hợp đồng rằng dữ liệu phải được lưu trữ không phải dưới định dạng độc quyền chỉ một công ty đọc được, mà dưới định dạng mở mà nhiều hệ thống có thể cùng đọc và ghi, thì ngay cả sau khi hợp đồng kết thúc, việc chuyển dữ liệu sang hệ thống khác cũng trở nên tương đối dễ dàng. Tuy nhiên, việc sử dụng tiêu chuẩn mở không đồng nghĩa với việc các thiết kế đặc thù cho hệ thống đó, như bộ thực thể (ontology), sẽ tự động được chuyển

đi. Việc thay đổi vỏ chứa dữ liệu sang dạng mở và việc chuyển giao cấu trúc trí thức chứa bên trong vỏ đó vẫn là hai nhiệm vụ khác nhau.

Khái niệm tính khả di không phải là hoàn toàn không có trong luật pháp Liên minh châu Âu. Đạo luật Dữ liệu Liên minh châu Âu (Data Act, Quy định (EU) 2023/2854) được thông qua năm 2023 đã có sẵn các điều khoản xử lý việc chuyển đổi giữa các dịch vụ điện toán đám mây và điện toán biên. Đạo luật này quy định giảm dần phí chuyển đổi áp đặt khi người dùng điện toán đám mây chuyển từ nhà cung cấp dịch vụ này sang nhà cung cấp dịch vụ khác, và bãi bỏ hoàn toàn các loại phí này sau một thời hạn nhất định. Khác với CADA, Đạo luật Dữ liệu có điểm khác biệt là một đạo luật đã có hiệu lực.

Nếu hiểu CADA là một nỗ lực nhằm mở rộng nguyên tắc tính khả di của Đạo luật Dữ liệu này sang một lĩnh vực nhạy cảm hơn nhiều là mua sắm công, và theo một tiêu chuẩn nặng ký hơn nhiều là chủ quyền, thì mối quan hệ giữa hai đạo luật sẽ trở nên rõ ràng. Nếu Đạo luật Dữ liệu nhằm bảo vệ người dùng đám mây thương mại thông thường khỏi sự phụ thuộc nhà cung cấp (vendor lock-in), thì CADA nỗ lực mở rộng tấm lá chắn bảo vệ đó sang cả các cơ quan nhà nước và dịch vụ công.

Đây chính là điểm mà đề xuất CADA muốn giải quyết. Một trong những mục tiêu chính sách mà Ủy ban châu Âu nêu ra là các cơ quan công có quyền chấm dứt hợp đồng vì lý do chủ quyền, còn nhà cung cấp gánh chịu nghĩa vụ chuyển giao dữ liệu và giá trị cấu hình theo định dạng mở và có khả năng tương tác khi hợp đồng kết thúc. Báo cáo BISI tổng kết rằng một trong ba trụ cột của CADA là việc thể chế hóa nghĩa vụ về tính khả di này, với mục đích ngăn chặn tình trạng các cơ quan công bị ràng buộc vào một nhà cung cấp cụ thể và đánh mất năng lực thương lượng. Việc điều khoản này thực sự xuất hiện dưới tên gọi và số điều khoản nào trong quy định cuối cùng sẽ cần phải qua quá trình thẩm tra của Nghị viện châu Âu và Hội đồng châu Âu mới được xác định.

Những gì có thể xác nhận ở thời điểm hiện tại chỉ là thực tế Ủy ban châu Âu đã đưa điều khoản theo hướng này vào bản đề xuất, chứ không phải là thực tế đã có quy phạm đang được thi hành.

Mặc dù hình thái cụ thể của thời gian hỗ trợ chuyển đổi mà đề xuất đề cập vẫn chưa được hoàn thiện, nhưng chúng ta có thể hình dung qua trường hợp của các ngành công nghiệp khác đã thi hành chế độ tương tự. Chế độ chuyển mạng giữ số cho phép người dùng dịch vụ viễn thông đổi nhà mạng mà vẫn giữ nguyên số điện thoại, hay chế độ chuyển đổi tài khoản ngân hàng chuyển giao cả lịch sử thanh toán tự động khi thay đổi tài khoản là những ví dụ điển hình. Nếu áp dụng ý tưởng này vào việc chuyển giao dữ liệu của cơ quan công, nhiều khả năng sẽ cần đến

quy trình trong đó nhà cung cấp cũ và nhà cung cấp mới cùng vận hành song song hệ thống trong một khoảng thời gian nhất định để chuyển giao dữ liệu và công việc theo từng giai đoạn.

Để cơ chế này hoạt động, cần phải đáp ứng đồng thời hai điều kiện. Một là quy định rõ quyền chấm dứt hợp đồng về mặt pháp lý, hai là bảo đảm tính khả di về mặt kỹ thuật để có thể thực sự thực thi quyền chấm dứt đó. Nếu chỉ có điều khoản pháp lý mà định dạng dữ liệu vẫn đóng, cơ quan công quyền dù có quyền chấm dứt hợp đồng cũng không có cách nào để sử dụng quyền đó. Ngược lại, dù về mặt kỹ thuật có thể di chuyển dữ liệu, nhưng nếu hợp đồng vương phải điều khoản phạt vi phạm, cơ quan công quyền sẽ tiếp tục ở lại với hệ thống cũ vì chi phí trước mắt. Trường hợp của NHS là một ghi chép về sự thất bại, cho thấy điều gì sẽ xảy ra khi không có điều kiện nào trong hai điều kiện này được đáp ứng.

Ngay cả khi CADA thực sự được thi hành, việc liệu nó có được áp dụng hồi truy cho các hợp đồng đã ký kết hay không vẫn là một vấn đề khác. Thông thường, các quy định mới của Liên minh châu Âu được áp dụng ưu tiên cho các hợp đồng mới ký kết sau ngày có hiệu lực, còn các hợp đồng hiện hữu thường đi kèm thời gian ân hạn hoặc các điều khoản chuyển tiếp riêng. Trong quá trình đề xuất CADA được hoàn tất chính thức, cách thức quy định các điều khoản chuyển tiếp đối với các hợp đồng hiện hữu nhiều khả năng sẽ trở thành trọng tâm đàm phán giữa các quốc gia thành viên. Từ góc độ của các cơ quan công quyền vốn đã giao phó dữ liệu cho một nhà cung cấp nhất định trong nhiều năm, nếu quy định mới không có hiệu lực hồi truy, họ sẽ phải mất một thời gian dài mới cảm nhận được hiệu quả của nghĩa vụ khả di.

Ở thời điểm bắt đầu ký hợp đồng, những chi phí này thường rất khó nhận thấy. Người phụ trách mua sắm thường so sánh các nhà cung cấp dựa trên chi phí triển khai ban đầu và phí dịch vụ hàng năm, chứ ít khi tính toán trước cả chi phí trích xuất dữ liệu sau khi hợp đồng kết thúc. Sự bất cân xứng này tạo ra động cơ riêng cho các nhà cung cấp. Chiến lược đưa ra mức giá ban đầu thấp để giành hợp đồng, rồi sau đó tăng chi phí chuyển đổi để giữ chân khách hàng là hiện tượng thường thấy trong ngành điện toán đám mây, vốn đã được chỉ ra qua nhiều phân tích thị trường. Nghĩa vụ khả di của CADA có thể xem là một nỗ lực nhằm thay đổi chính cấu trúc động cơ này ngay từ giai đoạn trước hợp đồng.

Vấn đề này hiện lên gay gắt hơn ở các nước nhỏ so với các nước lớn. Các quốc gia thành viên đông dân và dồi dào tài chính có đủ khả năng thành lập riêng đội ngũ pháp lý và kỹ thuật chuyên trách để kiểm tra hợp đồng. Ngược lại, chính quyền địa phương hoặc các cơ quan công quyền quy mô nhỏ tại các nước thành viên nhỏ

thường không có đủ ngay cả nhân sự chuyên môn để thẩm định hợp đồng. Việc chấp nhận nguyên vẹn hợp đồng mẫu do nhà cung cấp đưa ra trước mắt sẽ thuận tiện hơn so với việc theo đuổi đàm phán. Khi sự bất cân xứng này tích tụ, dù quyền chấm dứt vì lý do chủ quyền có tồn tại trong bộ luật, khoảng cách vẫn xuất hiện giữa các cơ quan có đủ năng lực thực thi quyền đó và những cơ quan không có.

Theo logic tương tự như việc đề xuất CADA mở kênh phê duyệt đơn giản hóa cho các nhà cung cấp vừa và nhỏ, có ý kiến cho rằng việc chuẩn bị sẵn các yêu cầu khả di chuẩn hóa và mẫu hợp đồng cho bên cơ quan công quyền tham gia ký kết là giải pháp để thu hẹp khoảng cách về năng lực đàm phán.

Vấn đề chi phí chuyển đổi vẫn kéo dài ngay cả sau khi hợp đồng đã kết thúc. Tách biệt với việc chuyển dời dữ liệu, nhân sự phụ trách xử lý dữ liệu cũng cần thời gian và ngân sách để làm quen với hệ thống mới. Do chu kỳ ngân sách của các cơ quan công quyền thường được lập theo từng năm, họ gặp nhiều khó khăn trong việc bố trí ngay một lúc khoản chi phí chuyển đổi trải dài qua nhiều năm. Chính vì vậy, ngay cả khi quyền chấm dứt vì lý do chủ quyền tồn tại về mặt pháp lý, tại nhiều quốc gia đã ghi nhận những trường hợp trên thực tế phải gia hạn hợp đồng chỉ vì bộ phận ngân sách không thể gánh vác chi phí chuyển đổi. Việc đề xuất CADA quy định thời hạn hỗ trợ chuyển đổi song song với nghĩa vụ khả di được xem là thiết kế có tính đến rào cản thực tế này.

Việc luật hóa quyền chấm dứt vì lý do chủ quyền và nghĩa vụ khả di kéo theo một sự căng thẳng pháp lý khác. Chỉ thị Mua sắm Công của Liên minh Châu Âu (Directive 2014/24/EU) và Hiệp định Mua sắm Chính phủ thuộc Tổ chức Thương mại Thế giới mà Liên minh Châu Âu tham gia về nguyên tắc quy định cấm phân biệt đối xử bất công đối với các nhà cung cấp nước ngoài đủ điều kiện trong quá trình mua sắm. Ngoại lệ dựa trên lý do an ninh quốc gia và quốc phòng tuy có căn cứ tại Điều 346 của Hiệp định về Hoạt động của Liên minh Châu Âu, nhưng ngoại lệ này từ đầu được thiết kế như một trường hợp ngoại lệ chứ không phải một nguyên tắc.

Nếu CADA dẫn đến hiệu quả thực tế là loại bỏ các doanh nghiệp ngoài châu Âu khỏi quá trình mua sắm ở cấp độ cao hơn của SEAL, nhiều khả năng sẽ nảy sinh tranh chấp pháp lý xung quanh việc liệu sự loại bỏ đó có nằm trong phạm vi hợp pháp của ngoại lệ an ninh hay không. Sự căng thẳng này vẫn là vấn đề tiếp tục được mổ xẻ qua từng từ ngữ của điều khoản trong suốt quá trình CADA được Nghị viện Châu Âu và Hội đồng Châu Âu thẩm định.

Có một con số khác giúp hình dung mức độ nghiêm trọng của vấn đề này. Palantir đã thông báo trong báo cáo kết quả kinh doanh quý 2 năm 2026 rằng họ đạt tỷ lệ tăng trưởng doanh thu 93% so với cùng kỳ năm trước. Ngay cả khi các quốc gia châu Âu tuyên bố giữ khoảng cách với Palantir trong lĩnh vực an ninh và quốc phòng nội địa, các ngân hàng đầu tư cùng các công ty quản lý tài sản tại châu Âu vẫn rót hàng tỷ euro để gom cổ phiếu Palantir, theo báo cáo của cơ quan truyền thông Đức Netzpolitik. Sự mâu thuẫn này—đẩy ra khỏi cửa mua sắm công nhưng lại cho vốn vào qua cửa sổ thị trường tài chính—không thể giải quyết chỉ bằng một điều khoản pháp lý.

Cũng không được bỏ qua thực tế rằng nghĩa vụ khả di là một công cụ không phân biệt hướng đi. Quy định giúp chuyển đổi dữ liệu dễ dàng không chỉ mở đường chuyển sang các doanh nghiệp châu Âu, mà còn mở cả đường chuyển sang các doanh nghiệp Mỹ khác. Bản thân quyền chấm dứt vì lý do chủ quyền và nghĩa vụ khả di không phải là công cụ ưu đãi cho doanh nghiệp mang quốc tịch cụ thể, mà giống như một cơ chế nâng cao năng lực đàm phán tổng thể của các cơ quan công quyền. Để năng lực đàm phán đó thực sự dẫn đến kết quả chọn lựa các doanh nghiệp châu Âu, rốt cuộc các yêu cầu về quốc tịch và cấu trúc quản trị do hệ thống SEAL quy định phải đồng thời phát huy tác dụng.

Vẫn còn tồn tại khoảng cách giữa tuyên bố bảo vệ chủ quyền và năng lực cung ứng thực tế của các phần mềm thay thế do châu Âu sản xuất nhằm hậu thuẫn cho tuyên bố đó. Quyền chấm dứt và nghĩa vụ khả di của CADA là bước đi thể chế đầu tiên nhằm khóa lấp khoảng cách này. Việc liệu bước đi đầu tiên đó có thực sự phát huy hiệu quả trên thực địa mua sắm hay không sẽ bộc lộ qua kết quả thẩm định của Nghị viện Châu Âu và quá trình triển khai sau đó.

---

## **Căn cứ và tài liệu tham khảo**

1. Ủy ban Khoa học và Công nghệ Hạ viện Anh, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', House of Commons, năm 2026.
2. Novara Media, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, năm 2026.
3. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), ngày 7 tháng 7 năm 2026.
4. Palantir Investor Relations, 'Palantir Reports Q2 2026 U.S. Comm Revenue Growth of 149% Y/Y and Revenue Growth of 93% Y/Y', Palantir Technologies, năm 2026.
5. Jan Ebert, 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, năm 2026.
6. European Union, Regulation (EU) 2023/2854 (Data Act), Official Journal of the European Union, năm 2023.

## 5.1 Ý tưởng 'EuroStack' của Francesca Bria và rào cản đầu tư 300 tỉ euro

Francesca Bria là nhà kinh tế học người Ý, từng hoạt động với tư cách cố vấn cho Ủy ban Châu Âu. Bà từng giữ chức Ủy viên Đột phá Số tại Tòa thị chính Barcelona, dẫn dắt chính sách giúp thành phố tự quản lý dữ liệu do người dân tạo ra thay vì giao cho các doanh nghiệp tư nhân. Kinh nghiệm này trở thành điểm tham chiếu mà bà liên tục dẫn chứng khi thiết kế các chính sách số ở cấp độ Châu Âu sau này. Trong nhiều phát biểu và bài viết, Bria đã bày tỏ mối lo ngại rằng xu hướng chuyển giao hạ tầng công cộng cho các công ty công nghệ tư nhân Mỹ có thể làm rung chuyển nền tảng của nền dân chủ.

Các sự kiện được đề cập ở những chương trước của cuốn sách này, cụ thể là việc DGSİ của Pháp rút khỏi Palantir hay sự cố Anthropic chặn truy cập, có thể coi là những ví dụ cụ thể cho thấy mối lo ngại này không dừng lại ở sự trần trụi trừu tượng. Điểm mà Bria lặp đi lặp lại và nhấn mạnh khi thiết kế EuroStack cũng không phải là các điều khoản trong hợp đồng, mà là câu hỏi: ai mới là chủ thể sở hữu và kiểm soát chính bản thân hạ tầng đó.

Theo đưa tin của cơ quan báo chí điều tra Follow the Money, Bria thông qua một nghiên cứu riêng có tên 'The Authoritarian Stack' (Chống công nghệ chuyên chế) đã chỉ ra xu hướng các ngân hàng đầu tư và công ty quản lý tài sản Châu Âu cung cấp nguồn vốn quy mô lớn cho các doanh nghiệp Mỹ như Palantir. Bà đã chỉ ra mâu thuẫn trong việc các quỹ hưu trí và ngân hàng Châu Âu lại đi tài trợ tài chính cho chính các công ty đang xâm hại hạ tầng công cộng của nước mình. Lời chỉ trích này gắn liền với vấn đề dòng vốn đầu tư nội bộ Châu Âu sẽ được đề cập ở phần sau của mục này.

Thành quả chuyển hóa mối lo ngại này thành bản thiết kế cụ thể chính là báo cáo EuroStack. Tên chính thức của báo cáo là 「EuroStack – A European Alternative for Digital Sovereignty」, do Bria cùng Paul Timmers và Fausto Gernone đồng tác giả. Quỹ tư nhân Bertelsmann Stiftung của Đức đã xuất bản báo cáo này vào ngày 13 tháng 2 năm 2025. Bertelsmann Stiftung là quỹ phi lợi nhuận do tập đoàn truyền thông lớn Bertelsmann của Đức thành lập, từ lâu đã tài trợ cho các nghiên cứu chính sách xã hội và kinh tế của Châu Âu.

Việc quỹ này xuất bản báo cáo EuroStack có nghĩa là báo cáo không phải văn bản chính thức của Liên minh Châu Âu, mà là bản đề xuất độc lập do một quỹ nghiên cứu chính sách tài trợ. Cần phải làm rõ điều này trước tiên. EuroStack không phải

là luật hay chính sách được Liên minh Châu Âu thông qua. Đó là bản đề xuất chính sách do một quỹ tư nhân phát hành, trong đó các tác giả kêu gọi Liên minh Châu Âu và chính phủ các quốc gia thành viên hành động theo hướng này. Các con số và thiết kế được đề cập trong chương này đều là nội dung nằm trong bản đề xuất đó, cần đọc và phân biệt rõ ràng với ngân sách đang thực sự được giải ngân hay các quy phạm đã được ban hành.

Đạo luật Phát triển Đám mây và AI (CADA) được đề cập ở Chương 4 và báo cáo này nằm ở các tầng bậc khác nhau. CADA là đề xuất quy định do Ủy ban Châu Âu trình lên Nghị viện Châu Âu và Hội đồng Châu Âu, đang trải qua quy trình lập pháp chính thức. Trong khi đó, EuroStack là báo cáo chính sách của một quỹ tư nhân nằm ngoài quy trình đó. Nếu CADA giải quyết vấn đề xây dựng trung tâm dữ liệu trong lãnh thổ Châu Âu và xác định quốc tịch của công ty vận hành, thì EuroStack là ý tưởng tự chủ hóa toàn bộ bảy tầng với phạm vi rộng hơn nhiều, từ bán dẫn cho đến trí tuệ nhân tạo.

Dù hai văn bản cùng chia sẻ mục tiêu tự chủ công nghệ của Châu Âu, chúng lại có sức nặng pháp lý khác nhau: một bên là đề xuất quy định đang trong quy trình lập pháp, còn bên kia là bản đề xuất chính sách đưa ra định hướng từ bên ngoài quy trình đó.

Khi giải thích về ý tưởng EuroStack, Bria thường dùng phép so sánh với việc đưa vào sử dụng đồng tiền chung Châu Âu (đồng euro). Tương tự như cách Châu Âu dỡ bỏ rào cản tiền tệ và thiết lập một trật tự tài chính chung trong thời kỳ mỗi quốc gia thành viên còn dùng một đồng tiền riêng, mục đích của phép so sánh này là nhấn mạnh rằng trong lĩnh vực hạ tầng số, năng lực rải rác của từng quốc gia thành viên cũng cần được tập hợp lại làm một. Nếu nhớ lại rằng việc đưa đồng euro vào sử dụng đã đòi hỏi nhiều năm đàm phán và sửa đổi hiệp ước, ta có thể hiểu phép so sánh này mang ý đồ nhấn mạnh quy mô tích hợp to lớn mà EuroStack hướng tới.

Báo cáo chia nền tảng số của Châu Âu thành bảy tầng. Ở tầng thấp nhất là nguyên liệu thô cần thiết để sản xuất bán dẫn và pin, cùng với năng lượng và nước cần thiết để vận hành các trung tâm dữ liệu. Xếp trên đó lần lượt là tầng sản xuất chip bán dẫn, tầng lắp đặt mạng truyền thông băng thông rộng, tầng sản xuất cảm biến và thiết bị Internet vạn vật (IoT), và tầng vận hành hạ tầng đám mây. Trên cùng là tầng phần mềm và tầng dữ liệu - trí tuệ nhân tạo. Báo cáo khẳng định rằng nếu bất kỳ tầng nào trong số bảy tầng này bị nắm giữ bởi doanh nghiệp bên ngoài Châu Âu, sự tự chủ của các tầng còn lại xếp phía trên sẽ không thể trọn vẹn.

Đó là logic cho rằng dù có tự sản xuất bán dẫn trong nước, nhưng nếu các máy chủ chứa bán dẫn đó chỉ chạy trong các trung tâm dữ liệu thuộc sở hữu của công ty Mỹ, sự tự chủ cũng chỉ dừng lại ở mức một nửa.

Rất dễ hiểu nếu ví cấu trúc bảy tầng này với trình tự xây một ngôi nhà. Dù có dựng tường bằng vật liệu chắc chắn đến đâu, nếu phải mua mái nhà lợp lên trên theo bản vẽ của người khác, sự an toàn của toàn bộ ngôi nhà sẽ phụ thuộc vào tay người bán mái. Sự tự chủ mà báo cáo EuroStack đề cập cũng tương tự. Luận điểm của báo cáo là: ngay cả khi các doanh nghiệp Châu Âu sản xuất từ bán dẫn, mạng truyền thông cho đến đám mây, nhưng nếu vẫn phụ thuộc vào sản phẩm của doanh nghiệp Mỹ ở các mô hình trí tuệ nhân tạo và phần mềm quản lý dữ liệu chạy trên đó, thì thành tựu đạt được ở sáu tầng bên dưới có thể bị lung lay chỉ vì một tầng trên cùng.

Báo cáo cũng đề xuất năm dịch vụ chung cung cấp trực tiếp cho người dân bằng cách kết hợp bảy tầng này. Đó là: dịch vụ đám mây chủ quyền xử lý tính toán trong nội bộ Châu Âu, ví căn cước kỹ thuật số xác minh danh tính người dân, hệ thống thanh toán bằng đồng euro kỹ thuật số cho phép thanh toán không tốn phí ngân hàng, không gian dữ liệu liên hợp trao đổi dữ liệu an toàn giữa các quốc gia thành viên, và công cụ trí tuệ nhân tạo do chính Châu Âu thiết kế và vận hành. Cả năm dịch vụ này hiện đều là những lĩnh vực đang phụ thuộc vào dịch vụ của các công ty Mỹ hoặc các công ty ngoài khu vực, và báo cáo giải thích rằng việc xóa bỏ sự phụ thuộc này chính là mục tiêu thực tế của ý tưởng EuroStack.

Trong số năm dịch vụ, dịch vụ gắn liền nhất với đời sống hằng ngày của người dân là hệ thống thanh toán bằng đồng euro kỹ thuật số. Hiện nay ở Châu Âu, khi thanh toán bằng thẻ, thông tin giao dịch đó phần lớn đi qua mạng lưới thanh toán của các công ty thẻ Mỹ. Một phần đáng kể trong khoản phí mà các cửa hàng phải trả mỗi khi chấp nhận thanh toán bằng thẻ sẽ chảy về công ty sở hữu mạng lưới thanh toán này. Hệ thống đồng euro kỹ thuật số mà báo cáo đề xuất là ý tưởng đặt chính mạng lưới thanh toán này vào bên trong hệ thống Ngân hàng Trung ương Châu Âu, nhằm ngăn thông tin giao dịch lọt ra ngoài khu vực và thay đổi cấu trúc phí. Ví căn cước kỹ thuật số cũng ra đời từ nhận thức vấn đề tương tự.

Ý tưởng là xây dựng một phương thức xác minh danh tính do nhà nước trực tiếp quản lý, thay cho thực tiễn hiện nay khi người dân phải thông qua hệ thống đăng nhập của các tập đoàn công nghệ lớn (Big Tech) cụ thể để chứng minh danh tính trên mạng. Cũng cần lưu ý rằng trong số năm dịch vụ này, riêng khái niệm ví căn cước kỹ thuật số không phải là khái niệm lần đầu tiên được đề xuất trong báo cáo EuroStack. Liên minh Châu Âu đã thông qua Quy định Định danh Kỹ thuật số

Châu Âu năm 2024, hay còn gọi là eIDAS 2.0, bắt buộc các quốc gia thành viên phải cung cấp Ví định danh kỹ thuật số Liên minh Châu Âu cho người dân. Quy định này là luật đã được ban hành và đi vào hiệu lực độc lập với báo cáo EuroStack.

Báo cáo EuroStack không đề xuất bãi bỏ cơ chế hiện hành này để làm lại từ đầu, mà thiên về việc đưa xu hướng đang diễn ra này vào trong cấu trúc 7 tầng nhằm kết nối một cách hữu cơ với các tầng khác. Ba dịch vụ còn lại nằm ở tầng mà chính phủ và doanh nghiệp trực tiếp tiếp xúc. Dịch vụ đám mây chủ quyền có định hướng trùng với hệ thống cấp độ bảo đảm chủ quyền của CADA đã được đề cập ở Chương 4.

Khác với các sản phẩm đám mây được gọi là "dạng chủ quyền" mà Amazon Web Services hay Microsoft tung ra nhắm vào khách hàng châu Âu vốn có hạn chế là không chuyển giao cổ phần chi phối cho châu Âu như đã xem xét ở Chương 4, dịch vụ đám mây chủ quyền mà EuroStack đề cập chỉ các đám mây có bản thân quyền sở hữu thuộc về châu Âu. Không gian dữ liệu liên minh là kênh giúp chính phủ và doanh nghiệp các quốc gia thành viên trao đổi dữ liệu với nhau mà không cần đi qua đám mây của Mỹ. Ý tưởng này có cùng bản chất với dự án Gaia-X do Pháp và Đức khởi xướng vào năm 2019, ra đời trước cả CADA đã được bàn đến ở Chương 4.

Khác với Gaia-X vốn bị đánh giá là chỉ dừng lại ở nỗ lực chuẩn hóa tự nguyện không có tính ràng buộc pháp lý, báo cáo EuroStack đề xuất nâng cấp hệ thống chia sẻ dữ liệu này thành hạ tầng chung được ngân sách nhà nước hỗ trợ. Động cơ trí tuệ nhân tạo chủ quyền hướng tới mục tiêu thay đổi thực trạng các cơ quan công quyền과 doanh nghiệp châu Âu hiện phải phụ thuộc vào các mô hình ngôn ngữ lớn do Mỹ 또는 các doanh nghiệp ngoài khu vực phát triển.

Quy mô đầu tư do báo cáo đưa ra không hề nhỏ. Các tác giả ước tính việc xây dựng mới hạ tầng 7 tầng này mất khoảng 10 năm, và chỉ ra rằng cần tổng nguồn vốn lên tới 300 tỷ euro tính đến năm 2035. Ngoài ra, báo cáo cũng bao gồm đề xuất thành lập một quỹ công nghệ riêng biệt trị giá 10 tỷ euro làm vốn mỗi ban đầu. Chia 300 tỷ euro cho 10 năm đồng nghĩa với việc phải duy trì đều đặn khoản đầu tư trung bình 30 tỷ euro mỗi năm. Con số này là tính toán của các tác giả báo cáo, chứ không phải ngân sách được Liên minh châu Âu chính thức thông qua hay phân bổ.

Khi đặt con số này bên cạnh ngân sách thực tế mà Liên minh châu Âu đang vận hành, khoảng cách sẽ hiện rõ. Báo cáo do cơ quan nghiên cứu chính sách CERRE công bố vào tháng 9 năm 2025 cho biết, ngân sách phân bổ cho hạng mục chủ quyền kỹ thuật số trong Quỹ Cạnh tranh mà Liên minh châu Âu đang xúc tiến ở

mức khoảng 55 tỷ euro. So với 300 tỷ euro mà báo cáo EuroStack đòi hỏi, quy mô này thậm chí chưa bằng một phần năm. Quỹ Cạnh tranh là hạng mục ngân sách mà Liên minh châu Âu muốn lập ra nhằm tăng cường năng lực cạnh tranh công nghiệp và kỹ thuật số trong khung ngân sách đa niên tiếp theo bắt đầu từ năm 2028, và hiện vẫn chưa nhận được phê chuẩn cuối cùng từ các quốc gia thành viên và Nghị viện châu Âu.

Điều này có nghĩa là ngay cả bản thân khoản ngân sách này cũng chưa phải là con số đã chốt, và phần dành cho chủ quyền kỹ thuật số trong đó còn kém xa số tiền mà EuroStack yêu cầu. Ý nghĩa của sự so sánh này rất rõ ràng. EuroStack là một bản thiết kế chỉ ra phương hướng, chứ không có nghĩa là ngân sách để hiện thực hóa bản thiết kế đó đã được bảo đảm.

Những người tham gia thảo luận chính sách tại châu Âu, bao gồm bà Bria, chỉ ra rằng nguồn lực bù đắp khoảng cách vốn này nằm ở tiền tiết kiệm tư nhân chứ không phải ngân sách chính phủ. Theo đưa tin của trang tin EU Perspectives vào tháng 1 năm 2026, tổng số tiền gửi mà các hộ gia đình Liên minh châu Âu để trong các tài khoản ngân hàng tính đến năm 2026 vượt quá 30 nghìn tỷ euro. Theo con số được đề cập trong phiên thảo luận tại Hội nghị thường niên Diễn đàn Kinh tế Thế giới vào tháng 1 năm 2026, khoản tiền này gấp hơn hai lần tổng sản phẩm quốc nội của toàn Liên minh châu Âu. Vấn đề là dòng tiền này không hề di chuyển.

Theo nội dung đề cập trong cuộc thảo luận do trang Politico phiên bản châu Âu phản ánh ngày 4 tháng 6 năm 2026, trong khi có những quốc gia như Thụy Điển với hơn một nửa người dân đầu tư tiền vào cổ phiếu hay quỹ đầu tư, thì tại nhiều quốc gia thành viên lớn của châu Âu, tỷ lệ này chỉ dừng lại ở quanh mức 2%. Cuộc thảo luận chỉ ra rằng tiền nằm chết trong ngân hàng không thể chảy tới các công ty khởi nghiệp, còn khoản tiền thực sự đi đầu tư thì phần lớn lại hướng về các cổ phiếu công nghệ lớn của Mỹ.

Các quỹ hưu trí cũng gặp phải vấn đề tương tự. Theo nội dung được phân tích trong cuộc thảo luận phát sóng trên France 24 vào tháng 6 năm 2026, các quỹ hưu trí châu Âu bị ràng buộc bởi quy định giám sát ưu tiên tính an toàn, khiến việc rót vốn cho các doanh nghiệp công nghệ ở giai đoạn đầu phát triển gặp nhiều khó khăn. Các quy định như Solvency II, cơ chế giám sát bảo hiểm và hưu trí của Liên minh châu Âu, buộc các quỹ hưu trí phải duy trì tỷ trọng tài sản an toàn trên một mức nhất định nhằm tránh tổn thất đột ngột.

Mục đích của quy định này là bảo vệ tiền dưỡng già của người nghỉ hưu, nhưng rốt cuộc lại tạo ra tác động làm thu hẹp kênh dẫn vốn hưu trí vào các tài sản rủi

ro cao và lợi nhuận không chắc chắn như doanh nghiệp công nghệ ở giai đoạn đầu. Tình trạng tắc nghẽn dòng vốn này dẫn đến sự chảy máu chất xám. Cuộc thảo luận nói trên cũng nhắc tới làn sóng nhân lực công nghệ châu Âu di chuyển sang Thung lũng Silicon ở Mỹ do không tìm kiếm được nguồn vốn. Tài liệu làm việc kèm theo SWD(2026) 502 final do Ủy ban Châu Âu công bố cùng đề xuất CADA cũng thể hiện khoảng cách vốn này qua các con số.

Trong tổng lượng vốn đầu tư mạo hiểm trên toàn thế giới, châu Âu chỉ chiếm tỷ trọng 5%, trong khi Mỹ chiếm tới 52%. Trong bài diễn thuyết tại CEPS vào năm 2024, bà Bria đã chỉ ra rằng một phần lớn các công ty khởi nghiệp thành công ra đời ở châu Âu khi bước vào giai đoạn mở rộng quy mô đã bị vốn nước ngoài thâm tóm và chuyển ra ngoài châu Âu.

Từ nhận định này, bà Bria đã kiến nghị cải cách hệ thống thuế nhằm định hướng tiền gửi ngân hàng và tài sản hưu trí chảy vào các doanh nghiệp công nghệ châu Âu. Các biện pháp được đề xuất bao gồm giảm thuế cho người dân rót vốn vào doanh nghiệp công nghệ trong nước thay vì tích trữ tiền tiết kiệm lâu dài, hoặc nới rộng hạn mức đầu tư vào tài sản rủi ro của các quỹ hưu trí. Việc các đề xuất này có được thể chế hóa thành luật thực tế hay chưa vẫn chưa thể xác định trong phạm vi tài liệu mà cuốn sách này tiếp cận. Logic của báo cáo là nếu muốn bù đắp phần lớn trong số 300 tỷ euro mà báo cáo EuroStack yêu cầu bằng nguồn vốn tư nhân chứ không phải ngân sách chính phủ, thì việc cải cách thuế như vậy phải đi trước một bước.

Không phải nguồn vốn hoàn toàn đứng yên. Theo tin đưa ngày 4 tháng 6 năm 2026 của trang tin kinh tế tiếng Pháp Ecoquick, Liên minh châu Âu đã chốt kế hoạch đầu tư 20 tỷ euro vốn công để xây dựng các đại công xưởng trí tuệ nhân tạo (Gigafactory). Trong thông báo ngày 1 tháng 7 năm 2026, Văn phòng Thủ tướng Tây Ban Nha cho biết đã phê chuẩn thỏa thuận phân bổ 720 triệu euro ngân sách công để xây dựng đại công xưởng trí tuệ nhân tạo tại quốc gia này. Trang tin Startup Online ngày 21 tháng 5 năm 2026 cũng phản ánh rằng Quỹ Scale-up Europe quy mô 5 tỷ euro do công ty quản lý tài sản EQT của Thụy Điển vận hành dự kiến bắt đầu giải ngân từ mùa thu năm 2026.

Quỹ này phối hợp hoạt động cùng Quỹ Công nghệ sâu (Deep Tech Fund) trị giá 1 tỷ euro do Ngân hàng Phát triển Đức KfW thành lập.

Ngay cả khi cộng tất cả các khoản chi tiêu thực tế này lại, tổng số 20 tỷ cùng 720 triệu và 5 tỷ vẫn chưa đạt tới 30 tỷ euro. Con số này chỉ bằng khoảng một phần mười so với mức 300 tỷ euro mà báo cáo EuroStack đòi hỏi. Việc Liên minh châu

Âu cùng một số quốc gia thành viên thực sự mở hầu bao là có thật, nhưng quy mô đó vẫn còn kém xa để lấp đầy bản thiết kế mà bà Bria đưa ra.

Khi đặt những con số này cạnh nhau, bản chất của vấn đề trở nên rõ ràng hơn. Tiền gửi ngân hàng của các hộ gia đình trong Liên minh châu Âu vượt quá 30 nghìn tỷ euro, trong khi khoản đầu tư mà báo cáo EuroStack yêu cầu là 300 tỷ euro. Tính toán thuần túy trên mặt số liệu, điều này có nghĩa là chỉ cần 1% số tiền gửi này được chuyển sang đầu tư công nghệ thì đã đủ đáp ứng toàn bộ số tiền mà báo cáo yêu cầu. Vấn đề nằm ở chỗ các động lực và cơ chế để dịch chuyển 1% này vẫn chưa được hoàn thiện. Bản chất của khoảng cách này nằm ở việc thiếu hụt chế độ thuế, các sản phẩm tài chính và niềm tin để chuyển số tiền đó từ tiết kiệm sang đầu tư, chứ không phải do thiếu tiền.

Nếu khoảng cách này không được thu hẹp, phần lớn trong số bảy tầng mà EuroStack phác thảo sẽ không thể thoát khỏi giai đoạn bản vẽ thiết kế. Các tầng đòi hỏi khoản đầu tư ban đầu khổng lồ như bán dẫn hay trung tâm dữ liệu sẽ là những nơi chịu ảnh hưởng của sự thiếu hụt vốn này đầu tiên. Đây là lý do xuất hiện những ý kiến cho rằng phương thức phân bổ ngân sách riêng lẻ theo từng quốc gia thành viên như hiện nay khó có thể gánh vác một dự án quy mô 300 tỷ euro, và cũng là lý do vì sao Bria tìm cách huy động cả nguồn tiền tiết kiệm tư nhân lẫn tài sản quỹ hưu trí.

Việc Liên minh châu Âu sẽ tăng ngân sách cho chủ quyền kỹ thuật số lên bao nhiêu trong các cuộc đàm phán ngân sách tiếp theo bắt đầu từ năm 2028 được dự báo sẽ là bài kiểm tra tiếp theo nhằm đánh giá liệu ý tưởng EuroStack có thể chuyển từ bản thiết kế sang dự án thực tế hay không. Cho đến khi có kết quả của cuộc đàm phán đó, EuroStack vẫn là bản đồ chỉ hướng đi cho châu Âu, chứ chưa phải là một tòa nhà đã hoàn thành.

---

## **Căn cứ và tài liệu tham khảo**

1. Francesca Bria, Paul Timmers, Fausto Gernone, 'EuroStack – A European Alternative for Digital Sovereignty', Bertelsmann Stiftung, ngày 13 tháng 2 năm 2025, <https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty>
2. Johanna Bröer và cộng sự, 'Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?', CERRE Issue Paper, tháng 9 năm 2025, 17 trang.
3. Joana Soares, 'Your cloud data lives on American servers. Brussels is moving to act', EU Perspectives, tháng 1 năm 2026.
4. World Economic Forum, 'Is Europe's Tech Sovereignty Feasible?', WEF Annual Meeting 2026, tháng 1 năm 2026.
5. POLITICO Europe, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, ngày 4 tháng 6 năm 2026, <https://www.politico.eu/video/achieving-digital-sovereignty-a->

golden-opportunity-for-the-eu-politico/

6. FRANCE 24 English, 'Can Europe own its digital destiny? EU unveils tech sovereignty roadmap', FRANCE 24, tháng 6 năm 2026.

7. European Commission, SWD(2026) 502 final, Công báo Liên minh Châu Âu, ngày 3 tháng 6 năm 2026, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502>

8. Francesca Bria, 'EuroStack: a concrete pathway to European digital sovereignty and strategic autonomy', CEPS Think Tank, năm 2024.

9. Loïc Kraft, 'Souveraineté numérique : Bruxelles renâcle à imposer des contraintes trop fortes', Écoquick, ngày 4 tháng 6 năm 2026.

10. Văn phòng Thủ tướng Tây Ban Nha, 'The President calls for public-private partnership to drive forward Spain's artificial intelligence gigafactory', La Moncloa, ngày 1 tháng 7 năm 2026.

11. Ban biên tập Startup Online, 'Báo cáo nghiên cứu về năng lực tính toán, đám mây, mã nguồn mở và vốn cho chủ quyền kỹ thuật số Châu Âu', Startup Online, ngày 21 tháng 5 năm 2026.

## 5.2 Liên minh phần mềm thay thế: Arcadia và hàng hóa công nghệ thuật số mã nguồn mở

Hệ thống chỉ huy và điều khiển, thường gọi tắt là C2, là phần mềm thu thập và hiển thị các sự kiện diễn ra trên chiến trường lên màn hình, đồng thời chuyển lệnh của chỉ huy tới các đơn vị. Hệ thống này tổng hợp và hiển thị theo thời gian thực đơn vị nào đang ở đâu, mục tiêu nào đã được phát hiện và lệnh nào đã được hạ cho đơn vị nào. Nếu Hệ thống Thông minh Maven đề cập ở Chương 3 đảm nhiệm vai trò này ở cấp độ liên minh NATO, thì Arcadia là nỗ lực của Pháp nhằm thay thế vai trò tương tự bằng phần mềm của chính mình.

Pháp đang phát triển một hệ thống chỉ huy và điều khiển bằng trí tuệ nhân tạo dùng trong quân sự do nước này dẫn đầu để thay thế Hệ thống Thông minh Maven của Palantir. Tên của hệ thống là Arcadia. Theo thông tin đăng tải ngày 9 tháng 7 năm 2026 trên các phương tiện truyền thông quốc phòng Armees.com và Economie Matin, Arcadia là phần mềm chỉ huy chiến trường do một liên danh gồm Thales, Airbus, Safran và nhà phát triển mô hình ngôn ngữ lớn Mistral AI của Pháp cùng chế tạo. Các công ty khởi nghiệp phần mềm tác chiến như Command AI và Impact cũng tham gia liên danh này.

Mistral AI là nhà phát triển mô hình ngôn ngữ lớn được thành lập tại Paris vào năm 2023, được đánh giá là giữ vị trí hàng đầu trong số các doanh nghiệp trí tuệ nhân tạo tại châu Âu. Việc công ty này tham gia vào liên danh quân sự cho thấy ngành trí tuệ nhân tạo dân sự của châu Âu đang kết hợp với lĩnh vực quốc phòng.

Arcadia không phải là dự án bắt đầu từ con số không. Theo cùng báo cáo, Pháp trước đây từng xúc tiến hệ thống sở chỉ huy tác chiến SIA C2 hợp tác giữa Thales và Sopra Steria trong nhiều năm, nhưng dự án đã bị hủy bỏ do vấn đề không tương thích về kỹ thuật. Liên danh Arcadia đã rút kinh nghiệm từ thất bại này để thiết kế hệ thống theo dạng mô-đun ngay từ đầu. Hệ thống áp dụng giao diện lập trình ứng dụng mở (API) để các thành phần phần mềm do nhiều công ty khác nhau chế tạo có thể kết hợp với nhau, đồng thời đáp ứng tiêu chuẩn Mạng Sứ mệnh Liên quân (FMN) của NATO vốn hỗ trợ truyền thông vô tuyến giữa các lực lượng đồng minh.

FMN là quy chuẩn chung được quy định để các hệ thống chỉ huy và điều khiển khác nhau của các quốc gia thành viên NATO có thể trao đổi thông tin trong các chiến dịch liên quân. Mục đích của tiêu chuẩn này là làm cho thông tin mục tiêu mà lực lượng của một quốc gia xác định bằng hệ thống của nước mình có thể được

đọc dưới cùng một định dạng trên hệ thống của quốc gia khác tuân theo tiêu chuẩn FMN. Việc Arcadia đáp ứng tiêu chuẩn này đồng nghĩa với việc Pháp không từ bỏ khả năng chia sẻ thông tin với quân đồng minh dù sử dụng phần mềm độc lập của riêng mình. Đây là thiết kế nhằm thỏa mãn đồng thời quyền tự chủ thiết kế của quốc gia và khả năng tương tác với quân đồng minh.

Thiết kế mô-đun là phương thức mua các thành phần đã chuẩn hóa từ nhiều công ty khác nhau rồi lắp ráp lại, thay vì mua nguyên vẹn một sản phẩm hoàn chỉnh lớn. Ngay cả khi công ty chế tạo một thành phần nào đó đóng cửa hoặc chấm dứt hợp đồng, chỉ cần thay thế bằng thành phần của công ty khác phù hợp với cùng quy chuẩn thì toàn bộ hệ thống vẫn tiếp tục vận hành. Khác với dự án SIA C2 trước đây vốn bị trói buộc bởi thiết kế khép kín của một nhà cung cấp nhất định, Arcadia nhờ vào cấu trúc mô-đun này mà giảm thiểu rủi ro toàn bộ hệ thống bị chi phối bởi tình hình của một doanh nghiệp duy nhất.

CWIX là cuộc tập trận thường kỳ của NATO về khả năng tương tác của lực lượng liên quân, là nơi kiểm tra hàng năm xem các hệ thống vũ khí và thiết bị thông tin liên lạc do các quốc gia thành viên phát triển có thực sự kết nối được với nhau hay không. Việc thử nghiệm trong cuộc tập trận này xem phần mềm chỉ huy và điều khiển mới phát triển có thể thực sự thông tin liên lạc với các thiết bị khác của quân đồng minh hay không đã trở thành thông lệ. Arcadia đã được vận hành thử nghiệm lần đầu tiên tại cuộc tập trận này diễn ra ở Bydgoszcz, Ba Lan vào tháng 6 năm 2026. Theo thông tin từ báo chuyên ngành quốc phòng Defense News ngày 5 tháng 6 năm 2026, cuộc tập trận này là dịp để kiểm chứng khả năng xử lý dữ liệu của Arcadia trong môi trường thực chiến.

Điều này có nghĩa là hệ thống chưa được triển khai toàn diện vào thực chiến mà mới ở giai đoạn thử nghiệm hệ thống đang phát triển theo các tiêu chuẩn của NATO. Theo cùng báo cáo, Tướng Patrick Justel, Phó Tư lệnh Lục quân Pháp, đã phát biểu tại cuộc tập trận rằng việc chấp nhận phần mềm nước ngoài mà không qua kiểm chứng là hành động tự từ bỏ chủ quyền quốc gia, đồng thời giải thích rằng Arcadia là câu trả lời của Pháp đối với sự ưu việt về kỹ thuật quân sự của Mỹ.

Có sự khác biệt rõ rệt trong phương thức phát triển giữa Arcadia và Maven. Palantir chọn phương thức nhà cung cấp duy nhất, phát triển Hệ thống Thông minh Maven dưới dạng phần mềm thuộc sở hữu của riêng mình để cung cấp cho NATO. Ngược lại, Arcadia chọn phương thức liên danh, trong đó Thales, Airbus, Safran, Mistral AI và nhiều công ty khởi nghiệp chế tạo các phân hệ theo lĩnh vực chuyên môn của mình rồi kết hợp lại dưới dạng mô-đun. Đây là thiết kế nhằm ngăn không cho bất kỳ một công ty nào chi phối toàn bộ hệ thống. Phương thức

này có nhược điểm là có thể làm chậm tốc độ phát triển, nhưng cũng có ưu điểm là giảm rủi ro phụ thuộc toàn bộ cơ sở hạ tầng an ninh vào một doanh nghiệp duy nhất.

Xu hướng này không chỉ giới hạn ở Pháp. Theo tin từ The Next Web ngày 18 tháng 7 năm 2026, chính phủ Pháp và Đức đã cùng cam kết tạo ra một hệ thống cạnh tranh ở cấp độ châu Âu để đối đầu với phần mềm trí tuệ nhân tạo quân sự của Palantir. Việc cam kết này có dẫn đến kế hoạch phát triển chung cụ thể hay không, hay các nước chỉ dừng lại ở việc tiếp tục xúc tiến các dự án độc lập như Arcadia, hiện chưa rõ ràng dựa trên các tài liệu được xác minh trong cuốn sách này. Theo danh sách do công ty tư vấn Pathfinders Group tổng hợp vào tháng 4 năm 2026, ngoài các công ty tham gia liên danh Arcadia, còn có nhiều doanh nghiệp khác được nhắc đến như là sự thay thế cho Palantir tại châu Âu.

Điều này có nghĩa là thay vì xác định một bên chiến thắng duy nhất, một cục diện trong đó nhiều doanh nghiệp cùng cạnh tranh trong lĩnh vực riêng của mình đang được hình thành.

Cho đến nay, Arcadia là dự án do Pháp chủ trì và các công ty tham gia liên danh phần lớn cũng là các doanh nghiệp Pháp. Dù cuộc tập trận CWIX là một sự kiện đa quốc gia với sự tham gia của các nước thành viên NATO, bản thân Arcadia chưa được phê chuẩn làm tiêu chuẩn chính thức của toàn bộ NATO. Việc các quốc gia thành viên khác ngoài Pháp có thực sự đưa hệ thống này vào sử dụng hay mỗi nước sẽ dùng một hệ thống riêng do nước mình phát triển vẫn chưa được quyết định trong phạm vi tài liệu được xác minh trong cuốn sách này. Nếu các nước châu Âu phát triển riêng rẽ các hệ thống chỉ huy và điều khiển khác nhau, khả năng tương tác giữa các quốc gia châu Âu có thể lại trở thành một thách thức mới.

Vai trò của Safran trong liên danh này là điều đáng xem xét riêng. Theo thông tin đăng trên phương tiện truyền thông kinh tế Pháp L'Essentiel de l'Économie ngày 8 tháng 6 năm 2026, Safran, vốn khởi đầu là nhà sản xuất động cơ máy bay, đã liên tiếp thôn tóm các công ty liên quan đến phân tích thông tin từ năm 2022. Vào tháng 7 năm 2022, Safran đã mua lại Orolia, công ty cung cấp tín hiệu vị trí chính xác ngay cả trong môi trường bị gây nhiễu, với giá 101 triệu USD. Năm 2024, công ty sáp nhập Preligens, doanh nghiệp phân tích hình ảnh vệ tinh, với giá 220 triệu euro để thành lập bộ phận mới Safran.AI. Vào tháng 2 năm 2026, Safran mua thêm Syntony, công ty sở hữu kỹ thuật chống gây nhiễu trong không gian ngầm, và vào tháng 5 năm 2026, công ty mua lại bộ phận quốc phòng của Kayros, doanh nghiệp phân tích hình ảnh ra-đa.

Theo cùng nguồn tin, bộ phận Safran.AI có 300 kỹ sư, doanh thu năm 2025 tăng 65% so với năm trước và dự báo sẽ tăng trưởng 90% trong năm 2026. Phương tiện truyền thông này cho biết công cụ nhận diện mục tiêu ACE do bộ phận này phát triển cũng đang được sử dụng để ký kết các thỏa thuận phát triển chung với các đối tác ở Singapore, Canada và Ấn Độ. Ý nghĩa của danh sách các quốc gia hợp tác này cũng là điều đáng ghi nhận. Singapore và Ấn Độ là những quốc gia không thuộc Five Eyes - liên minh chia sẻ thông tin tình báo do Mỹ dẫn đầu - nhưng vẫn duy trì hợp tác an ninh với phương Tây.

Việc Safran bắt tay với cả những quốc gia này có thể xem là nỗ lực mở rộng một mạng lưới hợp tác tình báo riêng bên ngoài liên minh tình báo do Mỹ làm trung tâm. Trường hợp một doanh nghiệp vốn sản xuất động cơ máy bay lại liên tục mua lại các công ty phân tích thông tin trong vài năm để chuyển mình thành một công ty trí tuệ nhân tạo cũng cho thấy xu hướng các tập đoàn quốc phòng lớn của châu Âu nhanh chóng sở hữu năng lực phần mềm và dữ liệu thông qua thâu tóm thay vì tự phát triển.

Bên ngoài lĩnh vực quân sự, các động thái xoay quanh phần mềm nguồn mở đang được triển khai. Tài liệu công báo COM(2026) 503 final do Ủy ban Châu Âu phát hành ngày 3 tháng 6 năm 2026 ước tính rằng chi phí các nước thành viên Liên minh Châu Âu chi trả cho phí thuê bao phần mềm của Mỹ lên tới 264 tỷ euro mỗi năm. Cùng tài liệu này đã đề xuất chiến lược nguồn mở mang nguyên tắc "ngân sách công, mã nguồn công", tức là công khai miễn phí cho người dân mã nguồn của phần mềm được phát triển bằng ngân sách công nhằm cắt giảm chi phí đó.

Lý do chi phí này lặp đi lặp lại nằm ở hiệu ứng khóa chặt đặc trưng của ngành công nghiệp phần mềm. Khi một cơ quan chính quyền bắt đầu tạo và lưu trữ tài liệu bằng phần mềm văn phòng của một công ty nhất định, dù vài năm sau có muốn chuyển sang sản phẩm của công ty khác thì định dạng tài liệu và quy trình làm việc cũng đã gắn liền với phương thức của công ty đó, khiến chi phí chuyển đổi tăng vọt như hòn tuyết lăn. Gánh nặng chi phí chuyển đổi này lớn hơn cả phí thuê bao hàng năm, nên các cơ quan công thường chọn giải pháp gia hạn hợp đồng. Điều mà chiến lược nguồn mở nhắm tới chính là cấu trúc khóa chặt này.

Lập luận ở đây là nếu công khai mã nguồn để nhiều công ty cùng cạnh tranh trên một nền tảng mã chung, ta có thể ngăn chặn tình trạng bị phụ thuộc hoàn toàn vào một nhà cung cấp duy nhất.

Theo nguyên tắc này, chính phủ các nước Pháp, Đức, Ý và Hà Lan vào tháng 10 năm 2025 đã thành lập một Liên minh Cơ sở hạ tầng Kỹ thuật số Châu Âu có tên là Digital Commons EDIC. EDIC là viết tắt của Liên minh Cơ sở hạ tầng Kỹ thuật

số Châu Âu, một hình thức tổ chức pháp lý được áp dụng khi nhiều quốc gia thành viên hợp tác triển khai dự án chung. Thay vì từng chính phủ ký kết hợp đồng riêng rẽ, một tổ chức duy nhất này đại diện cho các quốc gia tham gia để tập hợp ngân sách và quản lý dự án. Trọng tâm của liên minh này là phần mềm hợp tác văn phòng openDesk, vốn được Bộ Nội vụ Liên bang Đức phê duyệt phát triển như một giải pháp thay thế cho Microsoft 365.

openDesk là bộ phần mềm tích hợp công cụ lưu trữ tệp Nextcloud, máy chủ email Open-Xchange, công cụ quản lý nội dung Drupal và ứng dụng nhắn tin phân tán Matrix làm một. Thay vì mỗi chính quyền địa phương tự chỉnh sửa mã nguồn riêng, họ cùng quản lý mã nguồn thông qua một kho lưu trữ chung gọi là openCode. Trang blog Cosinex, chuyên trang về mua sắm công của Đức, cho biết chiến lược nguồn mở này đang được thúc đẩy cùng với nguyên tắc hành chính mang tên "Once-Only" (Chỉ một lần). "Once-Only" là nguyên tắc cho phép các cơ quan chính quyền chia sẻ thông tin đã nộp với nhau để người dân hoặc doanh nghiệp không phải nộp lại giấy tờ hay thông tin trùng lặp cho nhiều cơ quan khác nhau.

openCode dùng để chia sẻ mã nguồn và Once-Only dùng để chia sẻ thông tin hành chính tuy xử lý các đối tượng khác nhau, nhưng đều xuất phát từ cùng một ý tưởng là cắt giảm trùng lặp và chia sẻ tài nguyên. Các báo cáo liên quan cho hay, phần mềm hợp tác La Suite của Pháp, openDesk của Đức và MijnBureau của Hà Lan đã thực tế trình diễn việc phần mềm của ba quốc gia khác nhau có thể trao đổi tài liệu mà không cần thông qua các dịch vụ đám mây nước ngoài. Ý nghĩa của buổi trình diễn này không hề nhỏ. Cho đến nay, để công chức từ các nước khác nhau gửi và nhận tài liệu, họ thường phải gom về cùng một tài khoản đám mây của Mỹ.

Việc chứng minh ba quốc gia có thể liên thông với nhau dù sử dụng các phần mềm khác nhau cho thấy các nước châu Âu có con đường đảm bảo khả năng tương tác mà không cần phải thống nhất về một phần mềm duy nhất.

Chiến lược nguồn mở này nhiều khả năng cũng sẽ gắn kết với hệ thống mức độ đảm bảo chủ quyền (SEAL) của CADA được đề cập ở Chương 4. Các phần mềm hành chính thông thường như openDesk hay La Suite rất có thể sẽ thuộc về cấp độ thấp hơn với độ nhạy cảm tương đối thấp trong hệ thống SEAL, trong khi phần mềm liên quan trực tiếp đến quốc phòng như Arcadia có thể sẽ chịu các yêu cầu nghiêm ngặt ở cấp độ cao. Tuy nhiên, việc phần mềm nguồn mở và hệ thống phân cấp SEAL thực tế kết nối với nhau ra sao là vấn đề sẽ được cụ thể hóa trong quá trình CADA chốt các điều khoản cuối cùng.

Cũng có những ví dụ ở cấp chính quyền địa phương. Theo dữ liệu do Cổng thông tin Interoperable Europe của Ủy ban Châu Âu tổng hợp, bang Schleswig-Holstein ở phía bắc nước Đức đã tiến hành loại bỏ hệ điều hành Microsoft cùng Outlook khỏi 25.000 máy tính công chức từ năm 2020 để chuyển sang LibreOffice. Theo thông cáo báo chí được chính quyền bang đưa ra ngày 4 tháng 12 năm 2025, việc chuyển đổi này đã giúp chính quyền bang tiết kiệm 15 triệu euro chi phí bản quyền phần mềm mỗi năm.

Thụy Sĩ còn đi xa hơn bằng việc lập pháp. Theo tin đưa ngày 4 tháng 12 năm 2024 trên báo Watson của Thụy Sĩ, quốc gia này đã thông qua Đạo luật về Phương tiện Điện tử cho Chính phủ Điện tử (EM BAG) vào năm 2024, quy định bắt buộc về nguyên tắc phải công khai mã nguồn mở cho mọi phần mềm được phát triển bằng ngân sách công. Theo luật này, Bộ Tư lệnh Không gian mạng thuộc Bộ Tổng Tham mưu Quân đội Liên bang Thụy Sĩ đã phát hành miễn phí phần mềm phân tích an ninh Loom tự phát triển cho khu vực tư nhân. Việc quân đội đưa phần mềm tự phát triển ra dưới dạng nguồn mở là rất hiếm hoi, do đó quyết định này cho thấy Thụy Sĩ muốn đẩy mạnh mức độ tự chủ công nghệ quốc gia tới đâu.

Xu hướng này nằm cùng một mạch với việc chuyển đổi sang ArgonOS của Tổng cục An ninh Nội địa Pháp (DGSI) và sự rút lui của Cơ quan Bảo vệ Hiến pháp Liên bang Đức được đề cập trong Chương 1. Nếu Chương 1 thảo luận về quyết định của các cơ quan tình báo nội địa nhằm chuyển giao các nhiệm vụ vốn do Palantir đảm nhận sang sản phẩm của nhà cung cấp khác, thì Arcadia và openDesk trong mục này lại có điểm khác biệt: đó là các dự án phát triển để bản thân châu Âu tự tạo ra phương án thay thế. Quyết định thay đổi nơi thu mua và công việc tạo ra chính sản phẩm có thể thay thế là những nhiệm vụ ở hai giai đoạn khác nhau.

Arcadia, openDesk và EM BAG là các chương trình hoạt động trên những tầng nấc khác nhau. Arcadia giải quyết phần mềm chỉ huy và điều khiển quân sự, openDesk xử lý phần mềm văn phòng cho hành chính công, còn EM BAG quy định nghĩa vụ công khai mã nguồn bằng pháp luật. Cả ba dự án này đều chia sẻ một điểm chung duy nhất: đánh giá rằng thay vì thuê sản phẩm thương mại từ doanh nghiệp nước ngoài, châu Âu cần tạo ra phần mềm có thể tự sở hữu và chỉnh sửa mã nguồn ngay tại châu Âu.

Vẫn còn phải chờ xem nhận định này sẽ lan rộng đến đâu. Trong khi có những trường hợp đạt được kết quả nổi bật như bang Schleswig-Holstein hay Quân đội Liên bang Thụy Sĩ, không phải tất cả các quốc gia thành viên Liên minh châu Âu đều đang chuyển sang mã nguồn mở với cùng một tốc độ. Các cơ quan chính quyền càng gắn kết sâu sắc với phần mềm của Microsoft hay Google thì chi phí

ban đầu cho việc chuyển đổi và gánh nặng đào tạo lại nhân viên càng lớn, và ý chí chính trị để chấp nhận gánh nặng này không được hình thành ở mức độ như nhau tại tất cả các quốc gia thành viên. Những gì Arcadia và openDesk thể hiện là khả năng, chứ không phải là sự chuyển đổi hoàn tất trên toàn châu Âu.

---

## **Căn cứ và tài liệu tham khảo**

1. Jean-Baptiste Le Roux, 'Cloud de combat : face à Palantir, la France veut faire émerger un champion national des logiciels militaires', *Economie Matin*, ngày 9 tháng 7 năm 2026.
2. Jean-Baptiste Leroux, 'IA de combat : face au Palantir, la France veut son Maven hexagonal', *Armees.com*, ngày 9 tháng 7 năm 2026.
3. Rudy Ruitenbergh, 'France to test its own AI-powered battlefield command in June NATO exercise', *Defense News*, ngày 5 tháng 6 năm 2026.
4. Ban biên tập L'Essentiel de l'Éco, 'Comment Safran devient un géant du renseignement par IA', *L'Essentiel de l'Éco*, ngày 8 tháng 6 năm 2026.
5. European Commission, COM(2026) 503 final, *Công báo Liên minh châu Âu*, ngày 3 tháng 6 năm 2026, <https://ec.europa.eu/newsroom/dae/redirection/document/129100>
6. Digital Independence Editorial, 'Digital Sovereignty in Europe', *Digital Independence*, ngày 16 tháng 2 năm 2026.
7. European Commission, 'Open source progress in Schleswig-Holstein', *Interoperable Europe Portal*, năm 2026.
8. Chính quyền bang Schleswig-Holstein, *Thông cáo báo chí*, ngày 4 tháng 12 năm 2025.
9. Ban biên tập Watson, 'Schweizer Armee setzt auf europäische Software statt Microsoft', *Watson*, ngày 4 tháng 12 năm 2024.
10. Ban biên tập TNW, 'France and Germany pledge to build a European rival to Palantir's military AI software', *The Next Web*, ngày 18 tháng 7 năm 2026.
11. Pathfounders Group, 'Here are the top five companies vying to take on Palantir in Europe', *Pathfounders Group*, tháng 4 năm 2026.
12. Wolf Witte, 'Vergabebeschleunigungsgesetz und digitale Souveränität 2026', *cosinex Blog*, ngày 21 tháng 5 năm 2026.

### **5.3 Chủ quyền kinh tế chống lại các tập đoàn đa quốc gia né thuế: Báo cáo CICTAR và việc bảo vệ tài chính công**

Chính phủ các nước Châu Âu hàng năm đang chi trả một khoản ngân sách mua sắm công đáng kể cho các doanh nghiệp Mỹ như Palantir. Ngày 5 tháng 8 năm 2026, một báo cáo phân tích xem khoản chi tiêu này quay trở lại xã hội Châu Âu dưới dạng thuế được bao nhiêu đã được công bố. Trung tâm Nghiên cứu và Trách nhiệm Thuế Doanh nghiệp Quốc tế (CICTAR) là tổ chức nghiên cứu chuyên theo vết cấu trúc né thuế của các tập đoàn đa quốc gia, từng công bố nhiều báo cáo phân tích thực tiễn thuế của các tập đoàn đa quốc gia trước Palantir. Lần này, họ thu hẹp đối tượng nghiên cứu vào Palantir.

Báo cáo này, được thực hiện với sự hỗ trợ của Liên đoàn Công đoàn Dịch vụ Công Châu Âu (EPSU), đã phân tích cấu trúc thuế của Palantir và cho rằng công ty này chỉ nộp một khoản thuế rất nhỏ so với lợi nhuận thu được từ các hợp đồng công. Nội dung này đã được trang báo điều tra Follow the Money tổng hợp và đưa tin trong bài báo ngày 5 tháng 8 năm 2026. EPSU là liên đoàn công đoàn cấp Châu Âu đại diện cho người lao động trong khu vực công. Xu hướng gia tăng mua sắm công từ các doanh nghiệp tư nhân, bao gồm cả Palantir, là vấn đề ảnh hưởng trực tiếp đến việc làm và ngân sách của khu vực công, do đó cần làm rõ rằng việc EPSU tài trợ cho cuộc điều tra này là sự hỗ trợ từ một bên có lợi ích liên quan.

Thực tế này không tự động làm vô hiệu hóa nội dung phân tích của báo cáo, nhưng đây là thông tin nền tảng đáng để người đọc tham khảo khi đọc báo cáo này.

Bối cảnh khiến báo cáo này đề cập đến trường hợp của Đức xuất phát từ các hợp đồng mua sắm thực tế của cảnh sát. Theo tin từ cơ quan truyền thông Đức RepNet Germany, cảnh sát một số bang của Đức, bao gồm cả bang Hessen, đã sử dụng phần mềm của Palantir để theo dõi và phân tích các đối tượng đe dọa tiềm ẩn, trong tiếng Đức gọi là Gefährder. Báo cáo giải thích rằng việc tích lũy các hợp đồng như vậy ở nhiều bang đã trở thành cơ sở cho quy mô thất thu thuế tại Đức mà CICTAR ước tính.

Thuế suất thực tế là tỷ lệ giữa số thuế doanh nghiệp thực nộp chia cho lợi nhuận trước thuế. Dù thuế suất quy định trong luật có cao đến đâu, nếu số thuế thực nộp giảm xuống thông qua các khoản khấu trừ đa dạng và kỹ thuật kế toán, thuế suất thực tế cũng sẽ giảm tương ứng. Điều mà báo cáo CICTAR đặt ra vấn đề không

phải là Palantir đã vi phạm pháp luật, mà là công ty này đã sử dụng nhiều lớp kỹ thuật kế toán hợp pháp để hạ thấp thuế suất thực tế này. Trốn thuế (vi phạm luật thuế) và né thuế (giảm thuế trong phạm vi các thủ tục mà luật thuế cho phép) thuộc hai phạm trù pháp lý khác nhau. Điều báo cáo này tố cáo là trường hợp thứ hai. Sự phân biệt này cũng ảnh hưởng đến cách thức xử lý vấn đề.

Trốn thuế là đối tượng bị điều tra và xử phạt, nhưng né thuế lại không phải là vấn đề có thể ngăn chặn bằng cách xử phạt từng doanh nghiệp riêng lẻ. Điều này có nghĩa là cần có sự ủng hộ mang tính định chế, chẳng hạn như sửa đổi chính luật thuế, tái thiết lập các hiệp định thuế giữa các quốc gia, hoặc thay đổi các điều kiện của hợp đồng mua sắm công. Đề xuất BEFIT hay yêu cầu sửa đổi quy cách mua sắm công mà chúng ta xem xét ở phần sau của chương này chính là những biện pháp ủng hộ mang tính định chế như vậy.

Báo cáo CICTAR cho rằng thuế suất thuế thu nhập doanh nghiệp thực tế toàn cầu của Palantir năm 2025 chỉ dừng lại ở mức 1,4%. Theo báo cáo, Palantir đã đạt lợi nhuận trước thuế khoảng 1,66 tỷ USD trong năm 2025, nhưng số thuế thu nhập doanh nghiệp nộp trên toàn thế giới chỉ là 22,7 triệu USD. Các con số này dựa trên phân tích của CICTAR và Follow the Money, và cuốn sách này chưa kiểm chứng riêng báo cáo tài chính gốc của Palantir. Tuy nhiên, bản thân vấn đề mà luận điểm này nêu ra là điều cần xem xét.

Thỏa thuận này, do Tổ chức Hợp tác và Phát triển Kinh tế (OECD) khởi xướng với sự tham gia của hơn 140 quốc gia, được gọi là Trụ cột Hai (Pillar Two). Sau khi đạt được thỏa thuận khung vào năm 2021, thỏa thuận này đang lần lượt được cụ thể hóa vào luật nội địa của từng quốc gia tham gia. Mục tiêu của thỏa thuận này là áp mức thuế thu nhập doanh nghiệp tối thiểu 15% đối với các tập đoàn đa quốc gia dù họ hoạt động ở bất kỳ quốc gia nào. Nếu con số 1,4% mà báo cáo CICTAR đưa ra là sự thật, thì đây là kết quả đi quá xa so với tinh thần của thỏa thuận quốc tế này.

Một báo cáo riêng biệt do ITEP, cơ quan nghiên cứu chính sách thuế của Mỹ, công bố ngày 22 tháng 3 năm 2026 đã phân tích rằng Palantir thực tế hầu như không nộp thuế thu nhập doanh nghiệp liên bang tại Mỹ nhờ tận dụng khoản khấu trừ chi phí nghiên cứu và phát triển ngay lập tức theo đạo luật ưu đãi thuế được ban hành dưới thời chính quyền Trump.

Báo cáo CICTAR cũng giới thiệu các kỹ thuật kế toán mà Palantir sử dụng. Giữa trụ sở chính và các chi nhánh nước ngoài của tập đoàn đa quốc gia thường xuyên diễn ra giao dịch chuyển giá (transfer pricing). Đây là giao dịch mà chi nhánh gửi tiền cho trụ sở chính dưới danh nghĩa phí sử dụng công nghệ hoặc phí dịch vụ.

Tùy thuộc vào việc số tiền này được ghi nhận bao nhiêu mà lợi nhuận trên sổ sách của chi nhánh sẽ thay đổi đáng kể. Nếu chi nhánh gửi nhiều tiền cho trụ sở chính, lợi nhuận của chi nhánh sẽ giảm xuống, và số thuế thu nhập doanh nghiệp phải nộp tại quốc gia nơi chi nhánh đặt trụ sở cũng sẽ giảm tương ứng. Theo báo cáo, các công ty con của Palantir tại các nước Châu Âu thiết lập sổ sách kế toán theo cấu trúc chuyển doanh thu phát sinh từ hợp đồng về trụ sở chính tại Mỹ, và đổi lại chỉ nhận được một khoản phí dịch vụ nhỏ từ trụ sở chính tại Mỹ.

Trong cấu trúc này, lợi nhuận trên sổ sách của các công ty con tại Châu Âu được ghi nhận thấp hơn so với quy mô hoạt động thực tế. Báo cáo cho biết một phương thức khác đã được sử dụng tại Tây Ban Nha. Công ty con tại Tây Ban Nha đã chuyển 70% lợi nhuận thu được từ mua sắm công về trụ sở chính tại Mỹ dưới danh nghĩa phí sử dụng công nghệ, từ đó làm giảm đáng kể lợi nhuận chịu thuế của chi nhánh Tây Ban Nha. Thêm vào đó, báo cáo chỉ ra rằng chế độ thưởng bằng cổ phiếu—trả cho nhân viên bằng cổ phiếu của công ty thay vì tiền mặt—cũng được tính là chi phí theo luật thuế và được sử dụng để giảm thu nhập chịu thuế. Khi công ty phân phối cổ phiếu cho nhân viên, giá trị của cổ phiếu đó có thể được hạch toán vào sổ sách kế toán dưới dạng chi phí nhân công.

Vì chi phí nhân công được công nhận là chi phí hợp lệ theo luật thuế, nên chi phí này càng lớn thì lợi nhuận chịu thuế càng giảm. Trong ngành công nghệ, nơi thông lệ trả lương bằng cổ phiếu thay vì tiền mặt rất phổ biến, phương thức này thường được sử dụng như một công cụ giảm thuế hợp pháp.

Báo cáo cũng đưa ra các con số theo từng quốc gia. CICTAR ước tính rằng do cấu trúc kế toán này, thất thu thuế phát sinh tại Đức vào năm 2024 đạt 1,6 triệu euro, và số thuế thu nhập doanh nghiệp mà công ty con của Palantir tại Đức thực tế nộp trong năm đó chỉ dừng lại ở mức 640.000 euro. Tại Tây Ban Nha, báo cáo cho biết Palantir đã ký hợp đồng trị giá 16,5 triệu euro với các cơ quan an ninh quốc gia, nhưng số thuế thu nhập doanh nghiệp thực tế nộp chỉ vỏn vẹn 147.000 euro. Tất cả các con số này đều do CICTAR phân tích và đưa ra, không phải là tài liệu công bố chính thức của chính phủ các nước.

Tại Anh, một trường hợp riêng biệt đã được xác nhận. Theo tin đưa ngày 4 tháng 6 năm 2026 từ cơ quan truyền thông Novara Media, Cơ quan Y tế Quốc gia Anh (NHS) đã ký hợp đồng nền tảng dữ liệu tích hợp trị giá 330 triệu bảng Anh với Palantir. Hợp đồng này được gọi tên là Nền tảng Dữ liệu Liên bang (Federated Data Platform), là dự án nhằm tích hợp hồ sơ bệnh viện và khám chữa bệnh trên toàn nước Anh vào một hệ thống duy nhất. Palantir được chọn làm nhà thầu ưu tiên đàm phán cho dự án này vào năm 2023, và do đây là hợp đồng xử lý thông tin

y tế nhạy cảm của bệnh nhân nên ngay từ thời điểm được chọn, dự án đã gây ra tranh cãi trong giới y khoa và chính trường Anh.

Cũng theo báo cáo này, thuế thu nhập doanh nghiệp mà công ty con của Palantir tại Anh nộp cho cơ quan thuế Anh vào năm 2024 chỉ dừng lại ở mức 2 triệu bảng Anh. So với quy mô hợp đồng 330 triệu bảng Anh, số thuế thu nhập doanh nghiệp đã nộp chưa bằng 1/165 con số đó. Dĩ nhiên, việc so sánh trực tiếp tổng giá trị hợp đồng với số thuế thu nhập doanh nghiệp nộp trong một năm không phải là cách tính toán chính xác. Bởi lẽ không phải toàn bộ số tiền hợp đồng đều được tính là lợi nhuận của năm đó, và thuế thu nhập doanh nghiệp được tính trên lợi nhuận chứ không phải doanh thu. Tuy nhiên, các số liệu này cho thấy một thực tế là khoảng cách giữa hai con số đó lớn một cách đáng chú ý.

Trong một báo cáo riêng, Ủy ban Khoa học và Công nghệ thuộc Hạ viện Anh đánh giá việc vị thế của Palantir ngày càng gia tăng trong khu vực công là một điểm yếu khó chấp nhận.

Khi đặt các trường hợp của Đức, Tây Ban Nha và Anh cạnh nhau, một mô hình chung sẽ hiện ra. Cả ba quốc gia đều đã ký kết các hợp đồng công có quy mô đáng kể với Palantir, nhưng số thuế thu nhập doanh nghiệp thực tế thu được lại nhỏ hơn rất nhiều so với quy mô hợp đồng. Báo cáo CICTAR phân tích rằng việc cơ quan thuế của cả ba nước dù kiểm tra kế toán theo những phương pháp khác nhau nhưng vẫn cho ra kết quả tương tự cho thấy: cấu trúc kế toán này có khả năng không phải do sự giám sát lỏng lẻo của một quốc gia cụ thể, mà xuất phát từ chính sách kế toán được Palantir áp dụng chung cho nhiều nước.

Quốc gia mà báo cáo CICTAR coi là ngoại lệ là Pháp. Theo báo cáo, Cơ quan thuế Pháp đã yêu cầu Palantir ghi nhận đầy đủ lợi nhuận thu được tại Pháp vào sổ sách kế toán của chi nhánh Pháp, và kết quả là chi nhánh Palantir tại Pháp đã nộp 1,6 triệu euro thuế thu nhập doanh nghiệp vào năm 2024 với thuế suất thực tế là 33%. So với con số của các quốc gia khác, đây là một tỷ lệ cao hơn nhiều. Báo cáo giải thích rằng sự khác biệt này bắt nguồn từ việc thực thi thuế một cách chủ động của Cơ quan thuế Pháp. Pháp cũng là quốc gia đã áp dụng thuế dịch vụ kỹ thuật số riêng đối với các doanh nghiệp kỹ thuật số lớn có doanh thu tại nước này từ năm 2019.

Chế độ thuế nhắm vào các tập đoàn công nghệ lớn của Mỹ này từng nhiều lần gây ra mâu thuẫn thương mại với chính phủ Mỹ. Cách thức thực thi của Cơ quan thuế Pháp đối với Palantir cũng có thể được xem là sự tiếp nối của chính sách thuế nói trên.

Không chỉ dựa vào việc thực thi thuế của từng quốc gia thành viên, Ủy ban châu Âu cũng đang thúc đẩy một phương án riêng nhằm thống nhất chính cơ sở tính thuế của các tập đoàn đa quốc gia. Đề xuất mang tên BEFIT này đề ra giải pháp yêu cầu các tập đoàn đa quốc gia hoạt động trong Liên minh châu Âu xác định thu nhập chịu thuế theo một tiêu chuẩn chung duy nhất, thay vì tính thuế theo các phương pháp khác nhau ở mỗi quốc gia thành viên. Đề xuất này hiện vẫn đang trong quá trình xem xét của Nghị viện châu Âu và Hội đồng châu Âu, và được coi là một trong những nỗ lực nhằm giảm thiểu từ gốc rễ vấn đề chuyển lợi nhuận thông qua định giá chuyển nhượng mà báo cáo CICTAR đã chỉ ra.

Sau khi báo cáo này được công bố, giới công đoàn đã liên tục đưa ra phản ứng. Theo tin từ phương tiện truyền thông Đức Labournet Germany ngày 5 tháng 8 năm 2026, Tổng thư ký Liên đoàn Dịch vụ Công Quốc tế (PSI) Jan Willem Goudriaan cho biết cần dừng ngay thông lệ giao các hợp đồng mua sắm công cốt lõi của quốc gia cho các nhà cung cấp nước ngoài không bảo vệ ngân sách y tế công cộng và an sinh xã hội. Cùng bài báo cũng dẫn lời đại diện từ FNV, công đoàn lớn nhất Hà Lan, cho rằng không thể tiếp tục dung thứ cho thói quen của các doanh nghiệp hưởng lợi từ hạ tầng công cộng nhưng lại không nộp khoản thuế tương xứng. Các tổ chức đưa ra phản ứng này đang đề xuất đưa lịch sử nộp thuế vào hồ sơ yêu cầu kỹ thuật trong đấu thầu mua sắm công.

Cho đến nay, mua sắm công vẫn lấy giá cả và năng lực kỹ thuật làm tiêu chí đánh giá chính, và đề xuất ở đây là bổ sung thêm mức thuế thực tế mà doanh nghiệp đó đã nộp. Việc đề xuất này có được phản ánh vào các quy định mua sắm thực tế hay không vẫn chưa thể xác nhận trong phạm vi tài liệu mà cuốn sách này kiểm chứng.

Vấn đề thuế này cũng liên kết trực tiếp với khoảng cách đầu tư đã xem xét ở mục 5.1. Báo cáo Eurostack ước tính châu Âu phải huy động 300 tỷ euro cho đến năm 2035, trong khi ngân sách thực tế do Liên minh châu Âu phân bổ lại thấp hơn rất nhiều. Phía yêu cầu cải cách thuế cho rằng, nếu các doanh nghiệp ngoài khu vực bao gồm Palantir nộp thuế tương xứng với lợi nhuận thu được tại châu Âu như báo cáo CICTAR lập luận, thì nguồn thu thuế đó đã có thể đóng góp một phần vào nguồn vốn đầu tư mà Eurostack đòi hỏi. Tất nhiên, mối quan hệ nhân quả này là một lập luận chính trị của bên ủng hộ báo cáo CICTAR, chứ không phải là một thực tế được cuốn sách này xác minh riêng.

Vấn đề thuế này dẫn đến cùng một kết luận với vấn đề an ninh đã đề cập ở các chương trước, dù ở một tầng nấc khác. Chương 1 và Chương 4 đã bàn về vấn đề quyền kiểm soát phát sinh khi giao dữ liệu và vận hành hệ thống của quốc gia cho

các doanh nghiệp như Palantir. Vấn đề mà báo cáo CICTAR đặt ra là thực tế có bao nhiêu tiền từ các hợp đồng đó quay trở lại ngân sách quốc gia. Cơ quan An ninh mạng Quốc gia Ý cho biết họ đã cân nhắc cả hai vấn đề này để định hình chính sách theo hướng loại trừ các nền tảng gốc Mỹ khỏi các gói thầu mua sắm công trọng yếu của quốc gia.

Thực tế là hai căn cứ khác nhau – thuế và an ninh – cùng chỉ về một kết luận đang được nêu ra như lý do khiến các nhà hoạch định chính sách châu Âu không thể tiếp tục trì hoãn vấn đề này.

Dù là 300 tỷ euro mà Eurostack đòi hỏi, chi phí phát triển Arcadia và Offendesk, hay nguồn thu thuế mà CICTAR chỉ ra, cuối cùng tất cả đều quy về một câu hỏi. Đó là khi châu Âu muốn xây dựng một nền tảng công nghệ không phụ thuộc vào các công ty Mỹ, nguồn tiền để dựng nên nền tảng đó sẽ đến từ đâu? Dù là khơi thông nguồn tiền gửi đang nằm yên trong ngân hàng, phát triển phần mềm bằng ngân sách đã có sẵn, hay bịt kín các khoản thuế đang thất thoát, cả ba con đường đều hướng tới cùng một đích đến.

Dưới góc nhìn của người dân, đây không phải là một tranh cãi kế toán trừu tượng. Ngân sách mua sắm của đồn cảnh sát, bệnh viện hay Bộ Quốc phòng đều đến từ tiền thuế của người dân. Nếu một phần lớn ngân sách đó không quay trở lại kho bạc nhà nước dưới dạng thuế từ doanh nghiệp trúng thầu, nguồn tài chính dành cho các dịch vụ công sẽ bị giảm tương ứng. Trọng tâm của vấn đề mà CICTAR và Follow the Money nêu ra nằm ở chỗ chu trình tuần hoàn này hiện đang bị đứt gãy. Để chu trình nộp thuế, dùng thuế vận hành dịch vụ công, rồi dịch vụ công lại hỗ trợ hoạt động của doanh nghiệp có thể vận hành bình thường, cần phải có tiền để rằng doanh nghiệp ký hợp đồng mua sắm công phải nộp phần thuế chính đáng của mình tại quốc gia đó.

---

## **Căn cứ và tài liệu tham khảo**

1. Sebastiaan Brommersma, 'Tech giant Palantir accused of aggressive tax avoidance at Europe's expense', Follow the Money, ngày 5 tháng 8 năm 2026, <https://www.ftm.eu/articles/us-tech-giant-palantir-tax-avoidance-europe>
2. Rika Baack, 'Dubiose Praktiken: Palantir drückt sich vor Steuern', netzpolitik.org, ngày 5 tháng 8 năm 2026, <https://netzpolitik.org/2026/dubiose-praktiken-palantir-drueckt-sich-vor-steuern/>
3. Rika Baack, 'Big Data bei der Polizei', LabourNet Germany, ngày 5 tháng 8 năm 2026.
4. ITEP, 'Palantir Pays Zero Federal Income Tax Despite Explosive Growth, Largely Due to Trump Tax Law', ITEP Reports, ngày 22 tháng 3 năm 2026.
5. Joshua Carroll, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, ngày 4 tháng 6 năm 2026.

6. Ủy ban Khoa học và Công nghệ Hạ viện Anh, báo cáo, House of Commons, năm 2026.
7. Cơ quan An ninh mạng Quốc gia Ý, 'Sovranità digitale e IA: l'Italia tra autonomia e dipendenza', Chính phủ Ý, năm 2026.

## **Kết luận 1: Tuyên bố trước khi các giải pháp thay thế trưởng thành, vượt qua giai đoạn rủi ro 2-3 năm tới**

Ngày 15 tháng 12 năm 2025, Palantir thông báo đã ký một hợp đồng mới có thời hạn 3 năm với Tổng cục An ninh Nội địa Pháp. Chưa đầy sáu tháng sau hợp đồng này, vào ngày 16 tháng 6 năm 2026, Thủ tướng Pháp Sébastien Lecornu tuyên bố sẽ thay thế đối tác của hợp đồng này bằng công ty Pháp ChapsVision. Ngày hôm sau, tờ Le Monde đưa tin phía Palantir khẳng định hợp đồng đã gia hạn vẫn có hiệu lực về mặt pháp lý. Việc đưa ra tuyên bố và việc chấm dứt hợp đồng không phải là cùng một sự kiện. Trường hợp được đề cập ở Chương 1 của cuốn sách này thể hiện một cách cô đọng hình thái của những rủi ro chuyển đổi mà các chính phủ châu Âu sẽ phải quản lý trong 2 đến 3 năm tới.

Cần xem xét từ vấn đề mua sắm công trước. Bộ Nội vụ Pháp dự kiến sẽ mất từ 18 đến 24 tháng để triển khai phần mềm mới và chuyển đổi dữ liệu hiện có, trong khi các báo cáo khác cho rằng việc chuyển đổi hoàn toàn toàn bộ cấu trúc hợp đồng sẽ kéo dài từ năm 2027 đến năm 2029. Để lấp đầy khoảng trống này, Bộ trưởng Bộ Nội vụ Laurent Nuñez cho biết sẽ có một giai đoạn quá độ vận hành song song Palantir và ChapsVision cho đến năm 2027. Vấn đề tương tự cũng lặp lại tại Đức.

Vào tháng 5 năm 2026, Cơ quan Bảo vệ Hiến pháp Liên bang Đức đã quyết định chọn mua ArgonOS thay vì Palantir, nhưng để việc mua sắm này thực sự đi vào hoạt động, dự thảo luật sửa đổi dài hơn 700 trang quy định lại thẩm quyền của Cơ quan Tình báo Liên bang và Cơ quan Bảo vệ Hiến pháp Liên bang phải được thông qua trước. Tòa án Hiến pháp Liên bang Đức đã đặt thời hạn cho việc sửa đổi luật này là cuối năm 2026. Việc xác nhận mua sắm và thời điểm việc mua sắm đó thực sự đi vào vận hành bị ràng buộc vào các thủ tục khác nhau.

Bản thân các điều khoản hợp đồng cũng quyết định tốc độ chuyển đổi. Vào tháng 3 năm 2025, Bộ Nội vụ bang Baden-Württemberg đã ký hợp đồng triển khai phần mềm Gotham của Palantir với điều kiện thanh toán 25 triệu euro trong 5 năm mà không có điều khoản chấm dứt giữa chừng. Mặc dù 92% thành viên trong nội bộ Đảng Xanh thuộc chính phủ liên minh bang ủng hộ ý kiến phải dừng hợp đồng này ngay lập tức, nhưng một hợp đồng thiếu điều khoản rút lui đã không thể bị đảo ngược chỉ bằng sự phản đối chính trị. Hợp đồng này chứng minh bằng những con số rằng nếu không đưa sẵn điều kiện hủy bỏ vào hợp đồng mua sắm, nhà nước sẽ tự làm mất đi quyền năng thương lượng của chính mình.

Vấn đề di chuyển nhân lực và dữ liệu diễn ra bên ngoài hợp đồng. Các nhân viên của Tổng cục An ninh Nội địa Pháp đã quá quen thuộc với giao diện màn hình và cách thức thao tác của Palantir, và bản thân phương thức lưu trữ thông tin cũng được thiết kế theo tiêu chuẩn của hệ thống Mỹ. Để chuyển sang phần mềm mới, cần phải thực hiện theo trình tự các bước: điều chỉnh cách thao tác cũ cho phù hợp với màn hình mới, đào tạo lại nhân viên, thiết lập mới tuyến đường truyền dữ liệu, bảo đảm các cuộc điều tra đang diễn ra không bị gián đoạn, và kiểm chứng xem hệ thống có chịu được tải lượng công việc thực tế hay không. Quân đội Liên bang Đức cũng đang trải qua quy trình tương tự.

Vào tháng 4 năm 2026, Phó Đô đốc Thomas Daum thuộc Bộ Tư lệnh Không gian Mạng và Thông tin tuyên bố đã loại Palantir khỏi danh sách ứng viên của dự án đám mây quân sự pCloudBw. Sau đó, ba đơn vị gồm công ty Đức Almato, công ty khởi nghiệp Oakrist Technologies tại Berlin và công ty Pháp ChapsVision đã trải qua các đợt thử nghiệm kết nối dữ liệu thực tế trong mùa hè năm 2026. Đơn vị trúng thầu cuối cùng dự kiến sẽ được công bố vào cuối năm 2026. Việc loại bỏ Palantir và việc chọn ai thay thế vẫn là hai vấn đề riêng biệt.

Hà Lan đang đối mặt với một dạng rủi ro khác mang tên sự phân mảnh trong mua sắm công. Ngày 2 tháng 6 năm 2026, Thứ trưởng Quốc phòng Derk Boswijk đã phát biểu tại Hạ viện rằng ông sẽ thay thế Palantir bằng một giải pháp thay thế của châu Âu càng sớm càng tốt, đồng thời cho biết đặt mục tiêu 2 năm để tìm kiếm giải pháp thay thế có năng lực hoàn toàn tương đương. Tuy nhiên, trong văn bản trả lời Hạ viện sau đó của chính phủ, thay vì đưa ra thời hạn kết thúc cụ thể, họ chỉ dùng các cụm từ như xem xét giải pháp thay thế và giảm thiểu sự phụ thuộc. Bối cảnh đằng sau câu trả lời này là các hợp đồng ký với Palantir trong Bộ Quốc phòng được thực hiện riêng lẻ theo từng bộ phận, dẫn đến việc thậm chí không có một danh mục hợp đồng thống nhất ở cấp chính phủ.

Bản thân Thứ trưởng Boswijk cũng thừa nhận rằng nếu cắt đứt quan hệ ngay bây giờ, một khoảng trống an ninh có thể xuất hiện trong hệ thống tác chiến chiến đấu, hậu cần quốc phòng và xử lý thông tin. Chính phủ Hà Lan đã tự mình chứng minh cho thực tế rằng tốc độ của lời tuyên bố khác với tốc độ của việc thực thi.

Trong lĩnh vực tác chiến liên quân, hướng chuyển đổi lại đi theo chiều ngược lại. Năm 2025, Tổ chức Hiệp ước Bắc Đại Tây Dương thông báo đã đưa Hệ thống thông minh Maven của Palantir vào sử dụng tại Bộ Tư lệnh Tác chiến Liên quân. Tuyên bố đưa vào sử dụng này và phạm vi thực tế mà hệ thống đang vận hành tính đến năm 2026 vẫn là những vấn đề cần xem xét tách biệt. Tuy nhiên, như đã chỉ ra ở Chương 3 của cuốn sách này, có một thực tế rõ ràng là động thái loại bỏ

Palantir trong lĩnh vực tình báo an ninh nội địa và xu hướng duy trì vị thế của Palantir trong lĩnh vực liên minh quân sự đang diễn ra song song cùng một thời điểm.

Điều 2 và Căn cứ thứ 24 của Đạo luật Trí tuệ Nhân tạo Liên minh châu Âu loại trừ các hệ thống trí tuệ nhân tạo phục vụ mục đích quân sự, quốc phòng và an ninh quốc gia khỏi phạm vi áp dụng quy định. Điều này có nghĩa là việc các cơ quan tình báo nội địa từ bỏ Palantir không tự động dẫn đến việc thay thế mua sắm ở cấp độ quốc phòng và NATO. Đây cũng là lý do Bộ Quốc phòng Hà Lan nêu ra yêu cầu về khả năng tương tác (việc phải sử dụng cùng một hệ thống để trao đổi thông tin với các đồng minh NATO) làm rào cản cho sự chuyển đổi. Thêm vào đó, Đạo luật CLOUD của Mỹ mở đường cho các cơ quan điều tra Mỹ truy cập thông tin do các pháp nhân Mỹ xử lý, bất kể máy chủ đặt ở đâu. Trong giai đoạn chuyển đổi chưa hoàn tất, tầm ảnh hưởng của đạo luật này vẫn tiếp tục tồn tại.

Mức độ trưởng thành của nhà cung cấp thay thế cũng quyết định khoảng thời gian của giai đoạn chuyển đổi này. Kể từ khi thành lập vào năm 2019, ChapsVision đã trải qua hơn 25 thương vụ mua lại và đạt doanh thu 200 triệu euro vào năm 2025, nhưng so với một Palantir lâu đời, đây vẫn là một công ty đang trên đà phát triển. Các ứng viên cuối cùng của Đức là Almato và Oakrist Technologies cũng chỉ đến cuối năm 2026 mới quyết định được việc có triển khai thực tế hay không. Ủy ban châu Âu đã đưa ra mục tiêu tăng gấp ba lần năng lực trung tâm dữ liệu của châu Âu trong vòng 5 đến 7 năm thông qua Đạo luật Phát triển Đám mây và AI, nhằm đáp ứng nhu cầu của các doanh nghiệp và nền hành chính công cho đến năm 2035.

Tính đến tháng 8 năm 2026, đạo luật này mới chỉ là đề xuất quy định do Ủy ban châu Âu đưa ra và vẫn chưa được ban hành. Bản thân thời điểm hoàn thành kế hoạch mở rộng năng lực cung ứng đã hướng tới giữa những năm 2030.

Sự cố của Anthropic vào tháng 6 năm 2026 là bối cảnh của toàn bộ quá trình chuyển đổi này. Vào ngày 12 tháng 6, Chính phủ Mỹ đã ban hành chỉ thị kiểm soát xuất khẩu yêu cầu Anthropic chặn quyền truy cập vào Fable 5 và Mythos 5 đối với công dân nước ngoài. Quyền truy cập sau đó đã được khôi phục khi lệnh kiểm soát xuất khẩu được dỡ bỏ. Sự cố này chứng minh bằng thực tế khả năng nguồn cung có thể bị gián đoạn bất cứ lúc nào, chứ không hẳn là một sự phong tỏa vĩnh viễn. Trong khi Pháp, Đức và Hà Lan tìm kiếm các giải pháp thay thế với tốc độ khác nhau, khả năng này vẫn tồn tại mà không hề mất đi.

Điểm chung lộ diện qua các trường hợp được đề cập trong cuốn sách này là luôn có khoảng cách vài năm giữa ngày đưa ra tuyên bố và ngày hoàn tất chuyển đổi

thực tế mà không có ngoại lệ. Trong thời gian lấp đầy khoảng trống đó, các quốc gia không thể tránh khỏi việc vận hành song song cả công nghệ Mỹ lẫn các giải pháp thay thế của châu Âu.

---

## Căn cứ và tài liệu tham khảo

1. Palantir Technologies, 'Palantir Announces Renewal of Multi-Year Contract with the DGSI', Business Wire, 2025-12-15, <https://www.businesswire.com/news/home/20251215083215/en>
2. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, [https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice\\_6754592\\_7.html](https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html)
3. Markus Seyfferth, 'Wählt der BfV ArgonOS statt Palantir? Erstmals ja.', Dr. Web, 2026-05-01, <https://www.drweb.de/waehlt-der-bfv-argonos-statt-palantir-erstmals-ja/>
4. Không rõ tác giả, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, <https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518>
5. Không rõ tác giả, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, <https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html>
6. Không rõ tác giả, 'Bundeswehr Will Not Use Palantir for Military Cloud and AI Project; European Alternatives Examined', Grosswald, 2026-04-29, <https://www.grosswald.org/bundeswehr-rejects-palantir-military-cloud-ai-project-european-alternatives/>
7. Eglė Krištopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, <https://cybernews.com/tech/dutch-defense-palantir/>
8. Không rõ tác giả, 'Over twee jaar exit Palantir? Voorlopig blijft het bij intenties en verkenningen', iBestuur, 2026, <https://ibestuur.nl/markt-en-overheid/inkoop-en-aanbesteding/exit-palantir-blijft-het-bij-intenties-en-verkenningen>
9. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', NCIA, 2025, <https://www.ncia.nato.int/newsroom/news/nato-acquires-ai-enabled-warfighting-system>
10. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
11. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943, 2018, <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>
12. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
13. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, <https://www.anthropic.com/news/fable-mythos-access>
14. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, <https://www.anthropic.com/news/redeploying-fable-5>

## Kết luận 2: Con đường tự chủ bền vững duy trì tính mở (Resilient Openness)

Trong giai đoạn từ năm 2020 đến năm 2024, qua 4 năm, 5 cơ quan của Thụy Sĩ gồm Cơ quan Y tế Công cộng Liên bang, Cơ quan Thống kê Liên bang, Cơ quan Công nghệ Thông tin Liên bang, Cơ quan Thu mua Quốc phòng Armasuisse và Văn phòng Báo cáo Rửa tiền đã liên tục đưa ra quyết định không tiếp nhận Palantir. Thụy Sĩ không phải là quốc gia dỡ bỏ các chương trình đã đưa vào sử dụng như Pháp hay Đức. Đây là quốc gia mà số lượng các cơ quan ngăn chặn phần mềm bước qua ngưỡng cửa ngay từ đầu đã tích tụ qua thời gian, đến mức giờ đây thậm chí không còn cần phải thuyết phục mới.

Tháng 2 năm 2026, trang tin an ninh Gendata đưa tin rằng lý do Thụy Sĩ từ chối Palantir không phải vì hiệu năng kém, mà là do cấu trúc nội bộ độc quyền và thiếu minh bạch, quyền tài phán tư pháp nước ngoài cùng phương thức cập nhật từ xa được đánh giá là nguy cơ chủ quyền không thể kiểm soát. Phía Thụy Sĩ nhận định rằng việc giữ dữ liệu trong nước và đưa các điều khoản bảo hộ vào hợp đồng là không đủ để ngăn ngừa rủi ro này. Mặc dù vậy, điều đó không có nghĩa là Thụy Sĩ đóng cửa với toàn bộ công nghệ nước ngoài.

Đối tượng mà Thụy Sĩ thực sự lọc bỏ chỉ là một nhà cung cấp cụ thể mang tên Palantir, và tiêu chuẩn đánh giá của họ không nằm ở quốc tịch mà là vị trí lưu trữ dữ liệu, quyền tài phán cùng quyền kiểm soát cập nhật.

Động thái của Tây Ban Nha cũng cho thấy một lựa chọn mang tính thần tượng tự. Ngày 1 tháng 7 năm 2026, Văn phòng Thủ tướng Tây Ban Nha đã ban hành chỉ thị cho các doanh nghiệp công trực thuộc công ty mẹ quản lý vốn nhà nước, như công ty viễn thông Telefónica, công ty quốc phòng Indra và công ty đóng tàu Navantia, không được ký hợp đồng mới với Palantir. Dù vậy, họ không vô hiệu hóa các hợp đồng đã ký kết. Hợp đồng trị giá khoảng 16,5 triệu euro mà Trung tâm Tình báo Quân đội Tây Ban Nha đã ký với Palantir vẫn tiếp tục được duy trì cho đến tháng 11 năm 2026. Chính phủ Tây Ban Nha ngay từ bước thiết kế chính sách đã thừa nhận rằng việc ngăn chặn hợp đồng mới và việc chấm dứt hợp đồng hiện có là hai vấn đề hoàn toàn khác nhau. Ở chiều ngược lại là trường hợp của bang Baden-Württemberg.

Hợp đồng bị ràng buộc trong 5 năm với trị giá 25 triệu euro mà không có điều khoản rút lui này ngay cả 92% số phiếu phản đối từ nội bộ chính phủ liên bang cũng không thể đảo ngược. Tháng 2 năm 2023, Tòa án Hiến pháp Liên bang

Đức khi tuyên bố vi hiến đối với đạo luật làm cơ sở cho bang Hessen và bang Hamburg sử dụng hệ thống dựa trên Palantir trong hoạt động cảnh sát dự báo, cũng nhận định rằng phương thức phân tích diện rộng lịch sử liên lạc và thông tin cá nhân của công dân mà không có căn cứ pháp lý đã vi phạm quyền tự quyết thông tin. Khi hợp đồng không có lối thoát, cả quyết tâm chính trị lẫn phán quyết của tư pháp đều cần có thời gian mới có thể biến thành hành động.

Đặt các ví dụ này cạnh nhau, người ta thấy rõ hai thái cực—đóng cửa hoàn toàn và phụ thuộc vô điều kiện—đều sụp đổ theo những cách khác nhau. Hạn chế của xu hướng đóng cửa được thể hiện qua việc Thứ trưởng Quốc phòng Hà Lan Derk Boswijk tự mình thừa nhận. Ông cho biết nếu cắt đứt quan hệ với Palantir ngay lúc này, một khoảng trống an ninh có thể xuất hiện trong các hệ thống tác chiến combat, hậu cần quốc phòng và xử lý tình báo, đồng thời thừa nhận thực tế rằng trong lĩnh vực trí tuệ nhân tạo quân sự, Châu Âu chưa có phương án thay thế nào đạt trình độ tương đương. Việc đóng cửa mà không có năng lực hỗ trợ thì cũng chỉ dừng lại ở lời tuyên bố.

Ngược lại, giới hạn của sự phụ thuộc được phơi bày qua vụ việc kiểm soát xuất khẩu Anthropic vào tháng 6 năm 2026, cùng với Đạo luật CLOUD của Mỹ—đạo luật cho phép cơ quan điều tra Mỹ truy cập dữ liệu bất kể vị trí máy chủ nằm ở đâu. Những từ ngữ trong hiệp ước hay hợp đồng không thể ngăn cản sự phơi nhiễm này. Việc Đạo luật Trí tuệ Nhân tạo của Liên minh Châu Âu loại trừ các hệ thống AI phục vụ mục đích quân sự, quốc phòng và an ninh quốc gia khỏi phạm vi áp dụng cũng là bằng chứng cho thấy EU đã lựa chọn áp đặt các tiêu chuẩn riêng cho từng lĩnh vực thay vì dùng một quy tắc duy nhất cho tất cả.

Đề xuất Đạo luật Phát triển Đám mây và Trí tuệ Nhân tạo do Ủy ban Châu Âu đưa ra cho thấy con đường thực sự mà Châu Âu lựa chọn ở khoảng giữa hai thái cực. Tính đến tháng 8 năm 2026, đây không phải là luật đã được ban hành mà là dự thảo quy định của Ủy ban, đề ra mục tiêu nâng năng lực trung tâm dữ liệu lên gấp ba lần trở lên trong từ 5 đến 7 năm nhằm đáp ứng nhu cầu của doanh nghiệp và hành chính công trước năm 2035, coi đó là một phần trong kế hoạch hành động lục địa AI. Thiết kế 4 cấp độ đảm bảo chủ quyền và điều khoản quyền hủy hợp đồng vì lý do chủ quyền được đề cập trong Chương 4 của cuốn sách này chính là phương thức cô lập các lĩnh vực nhạy cảm nhất, đồng thời tiếp tục thu mua công nghệ nước ngoài ở các lĩnh vực còn lại nhưng chủ động bảo đảm trước quyền chấm dứt hợp đồng.

Đây có thể coi là nỗ lực dùng thể chế để ngăn chặn trước nguy cơ hợp đồng không có lối thoát mà bang Baden-Württemberg đã ném trái. Sáng kiến EuroStack của

Francesca Bria cùng các đồng nghiệp được đề cập ở Chương 5 của cuốn sách này cũng xuất phát từ sự trần trụi tương tự. Báo cáo nêu rõ rằng việc tái thiết hạ tầng kỹ thuật số trên toàn Châu Âu đòi hỏi một khoản đầu tư quy mô lớn kéo dài nhiều năm. Tổng kinh phí chính xác vẫn là nội dung cần kiểm tra lại dựa trên các hạng mục chi tiết trong báo cáo gốc.

Cách tiếp cận nhằm đồng thời nắm giữ tính mở và sự tự chủ này không phải là một kết quả đã hoàn tất, mà là một thử nghiệm đang tiếp diễn. Việc thử nghiệm đó có thực sự hiệu quả hay không phụ thuộc vào một số thời điểm cụ thể sắp tới. Quân đội Liên bang Đức sẽ chốt nhà cung cấp cuối cùng cho dự án pCloudBw vào cuối năm 2026. Quốc hội Liên bang Đức phải thông qua đạo luật quy định lại thẩm quyền của các cơ quan tình báo trước cuối năm 2026 theo thời hạn mà Tòa án Hiến pháp Liên bang ấn định. Bộ Nội vụ Pháp đã hứa sẽ vận hành song song Palantir và Hapsvision cho đến năm 2027. Hợp đồng Palantir của Trung tâm Tình báo Quân đội Tây Ban Nha sẽ đáo hạn vào tháng 11 năm 2026.

Liệu các mốc thời gian này có thực sự được tuân thủ hay không, và liệu các phương án thay thế của Châu Âu lấp vào vị trí đó có chứng minh được mức độ ổn định như Palantir trong thực tế hay không, chính là tiêu chuẩn tiếp theo để đánh giá liệu giải pháp dung hòa—không bế quan cũng không phụ thuộc vô điều kiện—này có thành công hay không.

---

## **Căn cứ và Tài liệu tham khảo**

1. Tác giả không xác định, 'Switzerland Ends Palantir Contract Over Data Sovereignty Risks', ZENDATA Cybersecurity, 2026-02-14, <https://zendata.security/2026/02/14/switzerland-ends-palantir-contract-over-data-sovereignty-risks/>
2. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, <https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns>
3. Tác giả không xác định, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, <https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518>
4. Bundesverfassungsgericht, 'Urteil vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20', Bundesverfassungsgericht, 2023-02-16, [https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216\\_1bvr154719.html](https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html)
5. Eglè Krištopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, <https://cybernews.com/tech/dutch-defense-palantir/>
6. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, <https://www.anthropic.com/news/fable-mythos-access>
7. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943, 2018, <https://www.congress.gov/bill/115th-congress/house-bill/4943/text>

8. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>
9. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, <https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada>
10. European Commission, 'Cloud computing', Digital Strategy, 2026, <https://digital-strategy.ec.europa.eu/en/policies/cloud-computing>
11. Francesca Bria et al., 'EuroStack: A European Alternative for Digital Sovereignty', 2025, [https://www.euro-stackreport.info/docs/EuroStack\\_2025.pdf](https://www.euro-stackreport.info/docs/EuroStack_2025.pdf)
12. Tác giả không xác định, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, <https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html>
13. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, [https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice\\_6754592\\_7.html](https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html)
14. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, <https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns>

Luật sư Kim Kyung-jin

[kimkj.com](http://kimkj.com)

© 2026 Kim Kyung-jin. All rights reserved.