數位主權的雙重結構

歐洲的去Palantir化與美國科技巨頭的鎖鏈

金京鎮 · 律師

目錄

第1章 歐洲去帕蘭提爾化與安保自立

1.1 法國對內安全總局（DGSI）的決斷：轉向 ChapsVision ArgonOS

1.2 德國聯邦憲法保衛局（BfV）的退出與從聯邦國防雲端計畫中排除

1.3 荷蘭國防部兩年內全面替代戰略與瑞士的徹底拒絕戰線

第 2 章 從虛擬走向現實：美國 Kill Switch 制裁衝擊

2.1 Anthropic「Fable 5」封鎖事件與盟友的警告

2.2 域外立法的陷阱：美國《雲端法案》與《外國情報監視法》第702條司法管轄範圍的真相

2.3 「實體隔離（Air-Gap）」與自主架構：超越合約條款的技術隔離

第3章 數位主權的雙重結構：國家自立與北約聯盟의 裂痕 -> 第3章 數位主權的雙重結構：國家自立與北約聯盟的裂痕

3.1 國內情報領域與軍事聯盟領域的差異

3.2 北約「Maven 智慧系統（MSS）」獲得完全作戰能力與互操作性的陷阱

3.3 歐盟《人工智慧法案》（AI Act）國安例外條款與監管盲區

第4章 歐洲的反擊：技術主權包裹法案與 CADA 的四階段框架

4.1 雲端與 AI 開發法（CADA）與資料中心加速區的規管創新

4.2 CADA 的四階段主權保證層級（Sovereignty Assurance Levels）設計

4.3 「主權事由解約權」（Sovereignty Termination Clause）與可攜性義務的制度化

第 5 章 歐洲堆棧與建立獨立替代生態系統的挑戰

5.1 弗朗切斯卡·布里亞的「歐洲堆棧（EuroStack）」構想與 3,000 億歐元的投資障壁

5.2 替代軟體聯盟：阿卡迪亞（Arcadia）與開源數位公共財

5.3 對抗避稅跨國企業的經濟主權：CICTAR 報告與公共財政保護

結論：從從屬的管理走向具備韌性的開放性

結論 1 替代方案成熟前的宣告，克服未來 2 至 3 年的風險區間

結論 2 保持開放性的具韌性自立（Resilient Openness）之路

1.1 法國對內安全總局（DGSI）的決斷：轉向 ChapsVision ArgonOS

法國對內安全總局是 2014 年重組負責國內情報業務的原有組織後成立的機構。監視恐怖威脅、因應外國間諜活動與網路攻擊是該機構的任務。對內安全總局自 2016 年起一直使用美國企業帕蘭提爾（Palantir）的資料分析軟體「哥譚」（Gotham）。引進的契機是 2015 年 11 月在巴黎發生的恐怖襲擊事件。對內安全總局當時急需一種能在單一介面上檢視恐怖組織通訊紀錄、行動路線與資金流向的工具，而帕蘭提爾的軟體填補了這個空缺。

法國政府並非從一開始就放任這種依賴。內政部於 2021 年發起公開招標專案 OTDH，旨在尋找能以單一國家系統處理各式龐大不同格式資料的法國企業技術。在這項招標中，除了 ChapsVision 之外，軍工巨頭泰雷茲（Thales）與資訊科技企業 Eviden 共同成立的合資公司 Athea，以及軟體企業 Blueway 也參與了競標。然而，沒有任何候選者能夠迅速發展到足以完整接管對內安全總局日常業務的程度。

對內安全總局於 2025 年 12 月選擇與帕蘭提爾續約，背景正是替代技術尚未在實務現場完全扎根的現實。

2025 年 12 月 15 日，帕蘭提爾宣布已與對內安全總局續簽多年期合約。這是一份為期 3 年的合約。然而，在新合約簽署還不到六個月的 2026 年 6 月，法國政府做出了與該合約正面衝突的決定。

起因是美國政府的處置措施。美國人工智慧企業 Anthropic 於 2026 年 6 月 9 日推出了旗下最先進的模型 Fable 5 與 Mythos 5。然而，僅在三天後的 6 月 12 日下午 5 時 12 分（美國東部時間），美國政府便以國家安全為由，下達出口管制指令，要求立即中斷外國籍人士對 Fable 5 與 Mythos 5 的存取。由於缺乏快速辨識使用者國籍的方法，Anthropic 選擇優先封鎖包括歐洲在內的全體海外使用者的連線存取。

正打算試用剛發布之最新模型的歐洲研究人員與行政機關，短短三天內就面臨存取管道被封鎖的困境。這項存取中斷雖然在 7 月 1 日前後出口管制解除後得以復原，但歐洲方面已親眼證實，同盟國僅憑一部法律就能切斷核心技術的存取服務。

在該事件發生的幾個月前，歐洲議會就已經確立了減少技術依賴的方向。歐洲議會於 2026 年 1 月 22 日以 471 票贊成、68 票反對、71 票棄權，通過了關於歐洲技術主權與數位基礎設施的決議案。該決議案對在雲端基礎設施、半導體、人工智慧及網路安全領域過度依賴少數外國業者的現狀表示憂慮，並提出了在公共採購中優先採用開源軟體的原則，以及設立規模達 100 億歐元的主權技術基金。

法國的決定，正是該決議案通過五個月後出現的個別國家層級執行案例。

法國政府在觀察此事態四天後採取了行動。總理塞巴斯蒂安·勒科爾尼（Sébastien Lecornu）於 2026 年 6 月 16 日宣布，將對內安全總局使用的帕蘭提爾工具替換為法國企業 ChapsVision 的 ArgonOS。發表時間恰在巴黎舉行的歐洲最大科技展 VivaTech 開幕前一天。而在前一天的 6 月 15 日，ChapsVision 剛剛入選法國創新企業指數 Next 40。

Next 40 是法國政府自 2019 年起營運的扶植名單，僅限企業估值超過 10 億歐元的獨角獸企業，或是三年內募集超過 1 億歐元投資的企業入選。這兩則消息在兩天內相繼出現，給人留下了這項決定是政府籌劃已久的印象。勒科爾尼總理表示無法再接受資訊科技領域的另一種戰略依賴，並表明仰賴盟友好意的時代已經結束。

這裡有一點需要釐清。宣布與合約終止並非同一件事。宣布次日的 6 月 17 日，《世界報》（Le Monde）報導指出，帕蘭提爾方面主張 2025 年 12 月續簽的合約在法律上依然有效。法國政府公開宣布新供應商，與既存合約實際終止，屬於不同的行政程序。法國內政部亦承認與帕蘭提爾簽署之展延合約的剩餘期限，並表示處理結算合約需要另行辦理行政程序。

實際的替換需要更多時間。法國內政部預估，將新軟體部署至情報第一線並轉移既存資料的工作需要 18 到 24 個月。另有報導認為，從整體合約結構來看，完全過渡將會在 2027 年至 2029 年之間完成。內政部長羅朗·紐涅茲（Laurent Nuñez）承諾，為了填補這段空窗期，將設立雙系統並行運作的過渡期直至 2027 年。轉移作業耗時甚久的原因，在於這並非僅是更換單一軟體的問題。

對內安全總局必須按順序執行五個階段：將過往習慣的操作方式轉移適應新介面、對人員進行重新培訓、建立新的資料傳輸路徑、確保進行中的偵查不致中斷，以及驗證系統能否承受實際業務負載。對內安全總局的人員早已熟悉帕蘭提爾的介面佈局與操作方式，且資料儲存方式本身就是依據美國系統的規格所建構。若急於切斷連結，恐有情報活動出現空窗期的風險，因此法國政府選擇了分階段轉型。

ChapsVision 正在開發的新平台預計將具備由人工智慧代理代為執行部分搜尋與分析的功能，而確認該功能在實際偵查現場能否如帕蘭提爾的工具般穩定運作的驗證程序，也是拉長轉移期間的因素之一。

支持這項決定的背後力量是「法國 2030」投資計劃。政府額外撥出 6 億 5,500 萬歐元，用於推動人工智慧領域的自主。其中一部分資金用於開發公務員專用的對話型人工智慧工具。2026 年 6 月 16 日，負責公職事務的部長達維德·阿米埃爾（David Amiel）宣布，將原本以一萬人規模試營運的聊天機器人「L'Assistant」擴大應用至全體高達一百萬名的公務員。第一階段擴建費用估計在 70 萬歐元至 75 萬歐元之間，開發工作則由法國人工智慧企業 Mistral AI 擔綱。

Mistral AI 執行長阿瑟·門希（Arthur Mensch）一直強調，歐洲必須擺脫租用美國雲端基礎設施的結構，擁有屬於自己的基礎設施。這番發言為對內安全總局的決定提供了邏輯上的強烈支持。

成為法國新供應商的 ChapsVision 是由奧利維耶·戴倫巴赫（Olivier Dellenbach）執行長於 2019 年創立的公司。戴倫巴赫執行長先前曾有在 2019 年將金融分析軟體公司 eFront 以 13 億美元出售給貝萊德（BlackRock）的經歷。ChapsVision 選擇了比起自主研發、更偏向透過併購擴展規模的策略。在接連收購顧客關係管理軟體企業 Coheris、零售資料企業 Octipas、電子商務企業 Sparkow 與行銷自動化企業 NP6 之後，又進一步收購了擁有網路安全、情報以及語音識別技術的 Bertin IT 與 Vecsys。

收購 Bertin IT 與 Vecsys 後，營收從 3000 萬歐元增至 4000 萬歐元，員工人數從 260 人增至 380 人。在接連完成二十五起以上的此類併購後，該公司獲得了法國國家投資銀行 Bpifrance 與 Tikehau Capital 的資金挹注，2022 年更追加籌集了 1 億歐元，2025 年單年營收已達到 2 億歐元。

ChapsVision 開發的 ArgonOS 是一款將格式各異的資訊匯集並進行分析的軟體。它不僅處理文件，還能在單一系統中處理影像、語音，乃至代表公開網路資訊的開源情報（OSINT）。該軟體運行於切斷外部通訊網路的實體隔離（Air-gap）環境，或是由國家直接管理的主權雲端之上。公司的股權全數由歐洲股東持有。這種所有權結構之所以重要，原因在於美國的《雲端法案》（CLOUD Act）。該法案規定，只要是由美國企業營運的服務，無論伺服器部位於哪個國家，都必須依據美國執法機構的要求提供資訊。

ArgonOS 並非美國企業，因而不在該法案的適用範圍之內。

對內安全總局選擇 ChapsVision 的程序同樣值得細查。該公司參與了法國內政部於 2021 年啟動的情報整合專案 OTDH 招標。OTDH 是一項旨在透過單一國家系統處理各式龐大資料的計畫，總預算編列約為 4000 萬歐元。經過三年多的審查，ChapsVision 於 2024 年底標下了負責整理原始資料的第 1 標案（Lot 1）承攬權。至於圍繞第 2 標案（Lot 2）的競爭則更為激烈。

在該標案的最後階段，僅剩泰雷茲（Thales）與 Eviden 的合資公司 Athea、軟體企業 Blueway 以及 ChapsVision 這三家業者；ChapsVision 於 2026 年 6 月在此角逐中再度勝出，順利拿下負責資訊視覺化與建模的第 2 標案承攬權，成為最終得標者。隨著這項決標，ArgonOS 的應用範圍超越了對內安全總局，進一步奠定了作為多家司法機構資料處理核心基礎系統的地位。

法國的這項決定也對鄰國產生了影響。德國聯邦憲法保衛局於 2026 年 5 月率先於法國，確定引進相同的 ArgonOS。該決定的背景與具體進展將於下一節探討。

在法國國家機構內部徹底清除美國技術，絕非短短幾個月內便能大功告成的任務。情報人員早已習慣的操作習慣、資料標準，以及現有合約的剩餘期限，均構成了重重阻礙。儘管如此，法國政府公開轉變政策方向的事實本身已無法逆轉。與帕蘭提爾（Palantir）的合約何時完全終止，以及向 ArgonOS 的實際轉移能否平順進行，仍是未來需要持續觀察與驗證的事實。

依據與參考文獻

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

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. 作者不詳, '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-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. 作者不詳, 'DGSI : Palantir éjecté, ChapsVision prend le relais en 2029', info.fr, 2026, https://info.fr/palantir-ejecte-dgsi-france-rompt-dependance-americaine-chapsvision/

10. 作者不詳, '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. 作者不詳, '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. 作者不詳, '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

13. ChapsVision, 'ChapsVision acquiert Bertin IT et Vecsys', ChapsVision, 2021, https://www.chapsvision.fr/acquisition-bertin-it-et-vecsys-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. 作者不詳, '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

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. 作者不詳, '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 德國聯邦憲法保衛局（BfV）的退出與從聯邦國防雲端計畫中排除

在德國，國內情報機構與軍方分別在不同時間點，但朝著相同方向與 Palantir 保持距離。這兩項決定並非單一事件，而是經過各自獨立程序的兩個事實。

德國聯邦憲法保衛局（BfV）是負責處理國內情報的最高機關。其職責為監控極端主義勢力的動向並防範外國間諜活動，地位與法國的國內安全總局相似。局長席南·澤倫（Sinan Selen）於 2025 年 12 月在德國內部會議上表示，安保機構必須更明確地建立歐洲觀點，並擺脫長期依賴。發表此番言論五個月後的 2026 年 5 月，聯邦憲法保衛局確定採購法國企業 ChapsVision 的 ArgonOS，而非 Palantir 的軟體。這被記錄為德國聯邦機構首次正式拒絕 Palantir 的案例。

聯邦憲法保衛局選擇的 ArgonOS 與前一節所說明的為同一款軟體。它能整合並分析不同格式的情報，同時具備追蹤公開網路資訊的公開來源情報（OSINT）功能。在德國方面值得關注的部分，是實際部署該軟體的過程中所建立的合作關係。ChapsVision 與長期管理德國警察資料庫 PIAV 的資訊科技公司 Rola Security Solutions 攜手合作。透過與已深植於德國治安網路的公司合作，使新軟體得以順暢融入現有體系之中。

這項採購並未立即部署於第一線。德國聯邦政府正在準備一份超過 700 頁的法律修正案，重新規定聯邦情報局（BND）與聯邦憲法保衛局的權限。該修正案賦予這兩個機構在面臨威脅情況時直接干預的權限，以及處理人工智慧與生物辨識情報的新手段，並包含強制要求聯邦憲法保衛局、各邦情報機構與軍事防諜組織軍事情報局（MAD）之間進行情報共享的內容。由於德國聯邦憲法法院已將修法期限明確定為 2026 年底，因此聯邦議會在夏季休會結束後將立即處理該法案。

包含 ArgonOS 在內的新分析工具，必須在這項法律框架完備後才能完全運作。在法律尚未完備的情況下，必須維持現有體系渡過過渡期。確定採購的事實，與該採購實際投入運作的時間點，就這樣被繫於不同的程序之中。

獨立於聯邦憲法保衛局的決定之外，德國聯邦軍在軍事領域另行採取了排除 Palantir 的措施。德國聯邦軍於 2017 年成立名為「網路與情報空間司令部」的獨立軍種，專責網路防禦與情報體系的運作。該司令部的湯瑪斯·道姆（Thomas Daum）海軍中將於 2026 年 4 月 28 日接受德國財經報紙《商報》（Handelsblatt）採訪時表示，目前完全沒有將 Palantir 用於軍事雲端計畫的打算。他指出，賦予外國民間企業員工存取德國國家資料的資格是不可想像的事。

這番發言使 Palantir 從聯邦軍推進的下一代國防雲端計畫 pCloudBw 的候選名單中排除。pCloudBw 是一項旨在將分散於各部隊的作戰資料與人工智慧處理能力整合至單一機密雲端上

的計畫，在 Palantir 被排除之前，曾是受評估的候選對象之一。

這項排除措施的背景源於對北大西洋公約組織（NATO）相關問題的疑慮。NATO 於 2025 年 3 月與 Palantir 簽訂短期合約，將 Maven 智慧系統引進指揮體系。Maven 是處理衛星影像情報並推薦打擊目標優先順序的軟體。然而，該軟體的日常運作與管理並非由軍人負擔，而是由 Palantir 的民間技術人員負責。德國國防當局認定，將戰術情報的管理權限交給盟國民間企業的結構可能會損害國家的防衛自主權。此外，美國的《雲端法案》（CLOUD Act）也成為一大障礙。

該法案規定，只要是由美國法人處理的資訊，無論伺服器部位於何處，美國調查當局皆有權存取。國防部認定無法接受德國聯邦軍的作戰計畫處於該法案射程範圍內的狀況。

排除 Palantir 後，聯邦軍在歐洲內部尋找替代候選者。在道姆中將的發言公開的 2026 年 4 月 29 日前後，聯邦軍已在廣泛評估德國企業 Helsing 的雲端與人工智慧體系 Altra、德國企業 SAP 的主權雲端體系 S3NS，以及法國企業 Atos 的 BullSequana XH3000。Altra 當時已部署於部分聯邦軍部隊，而 S3NS 則是軍工企業 Thales 用於轉移財務與採購業務的體系。在經過如此廣泛的篩選後，pCloudBw 計畫的最終候選者縮減為三家。

位於斯圖加特的 Almato 是德國企業 DATAGROUP 的子公司，具備德國聯邦資訊安全局（BSI）所要求的 VS-NfD 機密等級資料處理認證。位於柏林的新創企業 Orcrist Technologies 則展現了將不同格式的大規模情報整合為單一情勢意識畫面的技術。位於巴黎的 ChapsVision 也以 ArgonOS 參與此項競爭。這三家公司在 2026 年夏季期間進行了連動實戰資料的測試，最終得標者預計將於 2026 年底公布。

排除 Palantir 一事，與重新選定何人接手，就這樣仍是相互獨立的問題。

Palantir 執行長亞歷克斯·卡普（Alex Karp）對此決定做出即時回應。他在接受德國媒體《圖片報》（Bild）採訪時表示對此消息感到驚訝，並將德國的爭議比喻為關於魔法的故事。卡普執行長主張 Palantir 的技術已在烏克蘭戰場得到驗證，並提及自己與共同創辦人彼得·蒂爾（Peter Thiel）與德國結下的淵源。對此，德國數位部部長卡斯滕·威爾特貝格（Carsten Wildberger）反駁稱，不處於外國企業單方面控制下的自立，是國家安保中最應優先守護的條件。

德國對 Palantir 態度轉趨謹慎，司法部門的判決也起到了推波助瀾的作用。黑森邦於 2017 年引進 Palantir 的 Gotham，並以 hessenDATA 之名營運至今。德國聯邦憲法法院於 2023 年 2 月 16 日裁定，黑森邦與漢堡邦為了預測性警政而將該體系作為依據的法律條文違憲。法院認定，在缺乏法律依據的情況下廣泛分析公民的通訊紀錄與個人資料，侵害了資訊自我決定權。這項判決隨後成為德國各邦重新審視基於 Palantir 之體系的契機。

然而，並非所有的邦都朝著相同的方向行動。巴登-符騰堡邦內政部於2025年3月20日，在未事先與綠黨協商的情況下，簽署了引進帕蘭提爾（Palantir）Gotham 系統的合約。這份合約並

未包含得中途終止的條款，條件為5年內總計支付2,500萬歐元，每年約925萬歐元。參與邦聯合政府的綠黨內部，高達92%的人投票贊成應立即中止這項合約。然而，缺乏退場條款的合約無法單憑政治反對就被翻案，邦政府最終仍繼續執行該合約。

這個案例表明，若未在採購合約中預先納入解約條件，國家將會自行喪失談判籌碼。

此處有一點需要說明。歐盟的《人工智慧法案》（AI Act）將用於軍事、國防及國家安全目的的人工智慧系統排除在法規適用範圍之外。該法第2條與前言第24項將其依據歸因於各成員國各自承擔的國家安全責任，以及軍事活動本身的性質。換言之，聯邦憲法保衛局與聯邦國防軍排除帕蘭提爾（Palantir）的決定，並非遵循歐盟層級人工智慧管制規範的結果，而是德國作為單一國家，在採購與政治領域自行做出的選擇。

聯邦機關與邦政府這種步調不一的舉動，揭示了即使在同一個國家內部，維護主權的速度與方式也有所不同。聯邦憲法保衛局與聯邦國防軍在簽約前階段就排除了帕蘭提爾（Palantir），但巴登-符騰堡邦卻已被先前簽署的合約束縛住了手腳。

依據與參考文獻

1. 作者不詳, '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. 作者不詳, '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. 作者不詳, '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

7. 作者不詳, '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. 作者不詳, '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. 作者不詳, 'Geheimdienstreform: Zeitenwende für Spione', netzpolitik.org, 2026, https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/

10. 作者不詳, '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 荷蘭國防部兩年內全面替代戰略與瑞士的徹底拒絕戰線

荷蘭與瑞士以不同於法國和德國的方式與帕蘭提爾保持了距離。荷蘭試圖有計畫地撤除已在使用的軟體，而瑞士則連續多年選擇從一開始就不引進帕蘭提爾。

圍繞荷蘭國防部的討論，在調查報導媒體《Follow the Money》揭露國防部特種作戰司令部（SOCOM）也在使用帕蘭提爾，且軍事行動進行期間帕蘭提爾方能夠存取敏感資訊的事實後迅速升溫。《Follow the Money》在此前的採訪中也曾揭露荷蘭軍隊與警察多年來一直與帕蘭提爾進行秘密交易的事實。國防部方面澄清表示，帕蘭提爾員工的存取僅限於例外情況，且在監督下進行而非單獨作業，實際處理的並非機密資訊，而是虛擬或過期的資料。

然而，外國企業員工以任何形式存取機密資訊本身即對國家安全構成直接風險，這一指責並未平息。荷蘭國防副部長德爾克·博斯維克（Derk Boswijk）透露，在這份報導出來前一個月的2026年5月，他已在部門內部下達了減少使用帕蘭提爾的指示。他承認對帕蘭提爾的依賴令人擔憂，並表示已指示尋求歐洲替代方案。該事項引發爭議的另一個原因，在於帕蘭提爾甚至提供了利用人工智慧選定攻擊目標的功能。

博斯維克副部長於2026年6月2日在眾議院（Tweede Kamer）正式表示，將儘快以歐洲替代方案取代帕蘭提爾。他表示目標是在兩年內找到完全同等水準的替代品，但同時也承認，在軍用人工智慧領域目前尚無達到同等水準的歐洲替代方案。他還指出，若現在立刻切斷關係，可能會在作戰戰鬥體系、國防後勤與資訊處理方面產生縱使有限的安全空白，從而對立即切斷關係劃清了界線。

從宣布之後的實際進展來看，外界評價其進度相當緩慢。政府向眾議院提交的後續答覆中，並未給出具體的終止期限，僅包含了「檢討替代方案」與「降低依賴度」等表述。進展遲緩的原因有幾點。國防部內部與 Palantir 簽訂的合約是由各單位分別進行，政府層面甚至沒有一份統一的合約清單。這意味著無法一目瞭然地彙整進行中、預定執行或已結束的合約。此外，軍隊若要與 NATO 盟國交換情報就必須使用相同系統，這種相互操作性要求也成為一項阻礙。

負責邊境管理的皇家憲兵（Marechaussee）也在邊境監視系統中採用了帕蘭提爾的工具，因此這也是僅憑國防部一家的決定無法解決的問題。政治上雖然確定了方向，但將其付諸實行的具體動力依然微弱，這是追蹤採訪該事項的媒體所作出的共同評價。

瑞士則是另一個性質不同的案例。與法國或德國撤除已引進軟體做法不同，瑞士更接近於多家政府機構歷經數年接連決定不採納帕蘭提爾的情況。

瑞士聯邦公共衛生局於2020年4月至5月間，在管理COVID-19疫苗物流的招標中篩除了參標的帕蘭提爾。具體原因並未公開，但據傳負責部門對帕蘭提爾的參與本身提出了質疑。同年，瑞士聯邦統計局未回應帕蘭提爾方面的會面請求。瑞士聯邦資訊科技局在2020年至2021年期間與

帕蘭提爾進行了三次會議後，得出無須引進的結論。瑞士國防採購局（Armasuisse）於2020年，在軍事情報局資訊科技體系的招標中淘汰了帕蘭提爾。

淘汰原因為未滿足義務要件，而該要件具體為何則未予公開。

2022年10月，瑞士反洗錢申報處（MROS）接受了帕蘭提爾的軟體展示，但因缺乏引進的法律依據、認為存在違法疑慮而未予採用。這一趨勢持續到了2024年。帕蘭提爾歐洲業務負責人路易斯·莫斯利（Louis Mosley）於2024年6月在新加坡舉行的安全會議「香格里拉對話」上，親自會見瑞士軍隊參謀總長托馬斯·聚斯利（Thomas Süssli）並介紹了產品。

莫斯利指出瑞士軍隊對在資料中應用人工智慧與演算法感興趣，並提議實地展示產品，包括用於測量部隊備戰狀態的應用程式。瑞士軍隊參謀部收到該提議後撰寫了內部審查報告，於2024年12月初直接向聚斯利參謀總長報告。報告載明若引進帕蘭提爾的工具，瑞士軍隊的機密資訊可能會流向美國中央情報局（CIA）與國家安全局（NSA）的疑慮，瑞士軍隊便以此報告為依據，最終放棄了引進計畫。

隨著五個機構、跨越四年的拒絕不斷累積，在瑞士，不採納帕蘭提爾的態度已逐漸形塑為一種機構文化。帕蘭提爾在這整個期間積極敲響瑞士政府機關的大門，但最終連一份合約也未能拿下。據安全媒體 Zendata 於2026年2月14日報導，瑞士擊退帕蘭提爾的原因並非其性能不足。獨占且不透明的內部結構、外國的司法管轄權，以及透過遠端進行的更新方式，被評估為無法控制的主權風險。

瑞士方面的判斷是，僅憑將資料保留在瑞士境內並在合約中加入保護條款，不足以充分防範這一風險。

帕蘭提爾對報導這一拒絕趨勢的媒體報導也作出了強烈反應。瑞士調查報導媒體《Republik》於2024年12月發表了兩篇關於帕蘭提爾與瑞士的關係可能具危險性的文章。帕蘭提爾針對該報導提告《Republik》，要求刊登二十三則反駁聲明。蘇黎世商業法院在二十三則中僅裁定採認一則刊登，判給帕蘭提爾的損害賠償金也僅約9,000瑞士法郎。這一判決對帕蘭提爾在瑞士的信譽造成了又一次打擊。

大約在同一時期，西班牙也採取了新措施。西班牙首相府向國營企業控股公司（SEPI）旗下公營企業發布指令，要求不得與 Palantir 簽訂新合約，此消息於 2026 年 7 月 1 日經由西班牙媒體報導公開。這項措施旨在針對西班牙電信（Telefónica）、國防企業英德拉（Indra）以及造船企業納凡蒂亞（Navantia）等處理進階通訊網路與軍事情報的國營企業。不過，當局並未將已簽署的合約一律視為無效。西班牙軍事情報中心（CIFAS）與 Palantir 簽訂金額約 1,650 萬歐元的合約，仍將持續執行至 2026 年 11 月。

阻止新合約與切斷既有合約屬於不同層面的問題，這一事實同樣在西班牙的案例中獲得了印證。

將荷蘭、瑞士與西班牙放在一起對比，便顯露出歐洲與 Palantir 保持距離的方式並非只有一種。荷蘭對於已經滲透至國防體系各處的軟體，無法僅憑政治意志就輕易拔除。瑞士則因當初便將其擋在門外的一連串機構判斷有所累積，如今已達到幾乎不需要重新說服的狀態。西班牙則選擇封鎖未來簽訂合約的大門，同時靜待已簽署合約直到期滿。

無論採取哪一種做法，若要在不依賴美國技術的情況下運作安保體系，就必須事先準備好每一項合約條款與每一份機構間的協議，這一點 words 都是相同的。

依據與參考文獻

1. Eglė Kristopaitytė, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

2. 作者不詳, 'Defensie zoekt alternatief voor Palantir-software', Computable, 2026-06-03, https://www.computable.nl/2026/06/03/defensie-zoekt-alternatief-voor-palantir-software/

3. 作者不詳, '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. 作者不詳, '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. 作者不詳, '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. 作者不詳, '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. 作者不詳, '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 Anthropic「Fable 5」封鎖事件與盟友的警告

美國國防部與人工智慧企業 Anthropic 之間的摩擦，在 2026 年之前就已悄悄累積。Anthropic 在向政府機構提供自家的 AI 模型時，劃下了兩道明確的底線。其中一項是自家的模型不得搭載於直接針對人類進行殺傷的武器系統中；另一項則是模型不得用於針對本國公民的無差別秘密監視工作。這兩項條件是該公司在與政府簽訂合約之前就已表明的使用政策之延續。國防部高層並未接受這些條件。

他們要求獲得不受任何限制的全盤存取權限。將 AI 模型 directly 連接至武器目標選擇系統，或是毫無限制地掛載於篩選本國公民通訊與位置資訊的監視系統上，這便是國防部要求的實質內容。Anthropic 認為，一旦接受這些要求，自家的 AI 就會直接參與攸關人類生死存亡的決定或對本國國民的全盤監視。該公司堅持，即使承擔失去政府客戶的風險，也必須守住這兩道底線。雙方的談判未能縮小分歧。[1]

國防部見 Anthropic 拒不退讓，便將該公司指為本國軟體供應鏈的威脅因素。國防部官員正式將 Anthropic 定性為對國家安全構成致命威脅的「供應鏈風險企業」。這項認定在此之前是僅針對敵對國家之法人採取的強硬行政措施。民營 AI 企業遭到此類認定，在當時極為罕見。

川普政府於 2026 年 2 月 28 日下令禁止聯邦政府機構使用 Anthropic 的 AI 軟體。[1] 這項命令表面上看似處理採購法規的行政措施，實質上卻是施壓 Anthropic 接受國防部所要求之存取條件的手段。「供應鏈風險企業」這一認定並非只是聽起來沉重而已。獲得此認定的法人，在國防部採購體系內會被視為不可信賴的供應商進行管理；通常難以簽訂新合約，現有合約也會被列入重新審查的對象。

在此之前，該措施主要用於過濾與美國敵對國家有所關聯的法人。來自矽谷且享譽全球的 AI 開發商列入此名單，在此之前從未發生過。Anthropic 遭到此項認定本身，即表明國防部並非將這場衝突視為圍繞合約條件的談判，而是將其當作國家安全威脅問題來處理。

面對這股施壓，Anthropic 並未退縮，事態隨之轉移至法庭。聯邦法院法官於 2026 年 3 月 27 日並未站在國防部這一邊。法官認定國防部對 Anthropic 施加的壓力，屬於侵犯憲法第一修正案所保障之言論自由的政治報復。[1] 這是民間企業為了堅守自行訂定的使用條件而與公共權力正面衝撞，且該衝撞進而演變為法院裁決的事件。這項判決展現了在美國國內權力制衡機制仍在發揮作用的事實。

當行政部門對民間企業施加的壓力被判定為不當，司法部門得以出面阻擋。然而，這項司法制衡僅在美國國內有效。截至此時為止，這仍是發生在美國國內的行政部門與民間企業之爭，歐洲的政府或機構既無從觀望這場爭端結果，亦無途徑予以干預。

這場內部衝突並未止於國內訴訟。美國商務部於 2026 年 6 月 12 日頒布了限制人工智慧技術出口的命令。商務部提出以最高層級的國家安全維護作為此項措施的依據。[2][3] 該命令明確針對的目標是外國國籍使用者的存取。[2] 然而，Anthropic 並未具備可即時篩選連線者國籍的過濾系統。透過網際網路提供服務的公司，縱使能知曉註冊帳號的國家或付款所用信用卡之發卡國，也難以立刻確認每一位連線者的國籍。

因此 Anthropic 選擇了全面停止旗下效能最強大的模型「Claude Fable 5」與「Claude Mythos 5」的海外網際網路連線。在行政命令送達短短數小時內，包含歐洲在內的所有境外電腦連線便全數中斷。[1][5] 政府的指示雖係針對外國國籍人士，但實際上遭中斷的卻是與國籍無關的所有海外連線。此項措施與美國將特定企業或個人永久列入交易禁止名單的制裁，在性質上有所不同。

商務部採用的手段是以國家安全為由暫時限制特定技術出口的命令；此類命令法律上即便自發布起未明定期限，亦具備得隨政策判斷隨時撤銷的性質。然而對歐洲的使用機構而言，即便理解這種性質上的差異，連線遭到中斷當下的衝擊也並未因此減輕。

歐洲的多個行政機關與研究所，在未接獲事前警告的情況下，失去了日常使用的 AI 軟體。[1][5] 既沒有告知連線中斷原因的公告，也沒有設立可提出申訴的管道。即便是簽署了合約並持續支付使用費的機構，處境也沒有任何不同。繼續接受服務的權利，在供應商本國政府的出口管制判斷面前，使用合約顯得毫無力量。雲端服務條款或服務層級協定（SLA）並非能夠抵擋此類國家行政措施的保障機制。

歐洲的安全領域媒體將這起事件稱為「Fable 禁令（Fable-Ban）」進行報導。友邦的一紙行政命令可以在毫無事前協商的情況下，讓盟國的業務網路癱瘓，這一事實成為報導焦點。[5]

失去連線的並不只有政府部門。歐洲各國的行政機關以及大學、國家級研究所，日常業務中均在使用 Fable 5 與 Mythos 5，這些機構也在同一時刻以同樣的方式失去了這項工具。[8] 公共部門與學術研究部門共同經歷的這場中斷，成為深化各方認識的契機，讓人們意識到本次事件並非局限於特定部會或特定合約關係的問題，而是涵蓋了所有依賴美國技術的歐洲使用者階層。[8] 德國安全領域媒體 SecureCloud Blog 在一篇題為《美國軟體或被當作武器使用》的文章中，同時探討了圍繞 Palantir 的爭議與 Fable 5 的封鎖事件，並得出結論：歐洲所需要的並非對個別企業的不信任，而是「數位主權」。[5] 文章指出，無論與哪家公司簽訂合約，只要該公司的總部位於美國，就難以徹底擺脫相同的風險。[5]

這項封鎖持續了18天。美國政府直到2026年7月1日才撤銷出口限制措施。[3] Anthropic表示，在管制解除後，已進入恢復存取的程序。[4] 根據該公司的說明，因6月12日的措施而中斷的存取，並未隨著管制解除而立刻完全復原，而是以逐步進行的方式展開復原。[4] 政策翻轉並不意味著服務會在那一瞬間重新開啟。重新建立中斷的連線同樣需要時間。雖然封鎖在行政指令傳達後僅數小時內便告執行，但復原卻沒有那麼迅速。

要完全恢復至以往的狀態，還需要更多時日。儘管如此，事件的結局卻十分明確。連線遭到中斷，隨後又重新開啟。

在此必須確認的事實有兩點。第一，Fable 5與Mythos 5的海外連線確實遭到中斷。歐洲的多個政府機構與研究所在這18天內必須在缺乏此工具的情況下工作。第二，該項封鎖並未永久持續。美國政府改變了政策，連線隨之重新開放。若將此事件解讀為「美國人工智慧技術將不再供應給歐洲」的證據，並不符合事實。Anthropic在事件過後仍繼續在歐洲營運，歐洲的機構也重新簽署契約或延續既有合約。

反過來說，若將此事件當作什麼也沒發生過般輕描淡寫帶過，同樣不合事實。這18天內實際發生的中斷雖然未造成不可逆的損失，但在這18天裡需要使用連線的機構，除了尋求替代方案或推遲業務之外別無選擇。Fable 5事件真正展現的，是一種「供應隨時可能中斷，且決定中斷與重啟的權限並非掌握在使用國、而是掌握在供應商母國政府手中」的結構。引發這起事件的衝突，從一開始並非針對歐洲而起。

國防部與Anthropic之間的爭執，只是美國國內採購談判的延伸，歐洲與該談判毫無關係。然而，歐洲的政府與研究所卻被迫一同承擔了談判的後果。與自身無關的紛爭餘波竟然可能導致業務工具遭切斷，這一事實所帶來的不安感，甚至超越了身為相關當事國時的情況。下次究竟會因為什麼契機而以相同方式遭到斷連，歐洲的政府與機構根本無從預測。

這種結構在此之前對歐洲的政策制定者而言，只是一個遙不可及的概念。「數位主權」這個詞彙，過去僅會出現在學術研討會的發表論文或政策報告書的前言中。[1] 友邦政府在解決其國內政治紛爭的過程中所下達的一紙出口管制令，竟能在短短數小時內癱瘓同盟國政府機構的業務工具，這不再是理論，而是成為了實際發生的事實。[1][5] 商務部的命令所針對的目標雖是外國籍人士，但其後果卻是連帶切斷了同盟國政府與研究所的連線。

目標與結果之間的錯位，正是歐洲將此事件視為特別警告的原因。即便美國並非針對歐洲採取措施，但歐洲卻同樣落入該措施的射程範圍之內，這一事實本身就是問題所在。美國的出口管制通常是用於防止技術流向敵對國家的手段，而包括北大西洋公約組織（NATO）成員國在內的友邦，在慣例上一直與管制對象有所區分。然而在Fable 5事件中，這種區分在現實中並未得到遵守。

劃分友邦與非友邦的界線僅存在於政策意圖之中，並無過濾國籍的技術機制予以配套支撐。歐洲各國政府從此事件中所解讀出的，正是這道鴻溝。意圖上的區分與實際執行之間所產生的縫隙，光憑同盟國的地位是無法彌補的。

行動最迅速的國家是法國。法國內政部長塞巴斯蒂安·勒科爾尼在商務部下達出口管制令4天後的2026年6月16日宣布，將法國內務安全總局的情報分析系統從美國Palantir的軟體更換為法國企業Hapsvision開發的ArgonOS。[6] 這項宣布不應被解讀為與Palantir的合約當場結束。

Palantir與法國政府之間的合約在當時仍剩餘多年期限，若要終止合約，必須支付違約金並進行額外談判。

實際的系統替換同樣是宣布之後才進行的獨立過程。[7] 即便如此，法國政府在商務部命令下達後僅4天便提出此方向的宣布，這一事實展現了Fable 5封鎖事件在歐洲政府內部以多麼迅速的速度轉化為政策討論。法國只是在這股趨勢中第一個做出宣布的國家，並非唯一的國家。

在Fable 5遭到封鎖後的數月間，歐洲其他國家政府也接連展開重新檢視對美國技術依賴度的程序。[8] 雖然各國具體採取的途徑因國而異，但這次事件作為起點這一事實卻是共同的。

Anthropic的案例留給歐洲的教訓，並非「單一公司不可信賴」。Anthropic頂住了國防部的要求，堅守了自家設定的使用條款，法院也判決該公司勝訴。該公司為了守住「殺傷性武器」與「無差別監視」這兩條紅線所承受的壓力，反而證明了其對自身原則的忠實。被指為問題核心的並非Anthropic的態度，而是「只要美國政府有所意圖，任何美國企業的海外服務都能以相同方式被中斷」的結構本身。

今天雖然是國防部與Anthropic之間的衝突，但下次其他公司與其他衝突同樣可能導致相同的結果。無論該衝突是源於貿易紛爭、安全政策，亦或是如本次般源於政府與企業間的內部談判，結果皆然。歐洲的政府與研究所即便並非該衝突的當事方，卻站在了全盤承擔後果的一方。

18天這段時間對於實際業務停擺而言絕非短暫。同時，這段期間終將結束的事實也透過本次事件得到了確認。一旦美國政府改變判斷，連線便會重新開放。歐洲各國政府在此事件後開始重新審視本國技術採購政策的原因，正是在於這一點。無論在合約書中寫入多麼詳盡的條款，在供應商母國政府的決定面前，這些條款都將失去效力，這一事實透過此事件變得清晰明瞭。比起「連線遭到切斷」的事實，決定連線開始與結束的權限掌握在自己掌控之外這一事實，才是留存更久的深層問題。

因此，「Fable 5」事件在歐洲的政策文件中留下的，並非封鎖永遠持續下去的故事，而是封鎖隨時 possible 再次發生、且決定權掌握在其他國家政府手中的故事。即使在連線恢復之後，這起事件依然不斷被引用的原因就在於此。危機過去之後留下的問題，不是中斷了什麼，而是下次其他國家的政府是否還會做出相同的決定。只要歐洲無法自行掌控這個問題的解答，這長達18天的封鎖就不會是一次性的偶發事故，而是會作為可能重演的可能性留存下來。

依據與參考文獻

1. Centre for Future Generations, 'Enforcement spotlight, Spring 2026', Centre for Future Generations, 2026年春季號.

2. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026年6月12日, 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, 2026年7月1日, https://www.computerworld.com/profile/gyana-swain-2/

4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026年, 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, 2026年6月8日, 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, 2026年6月16日, 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, 2026年6月17日, 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. 「歐盟(EU)主要國家脫Palantir動向與數位主權化分析報告」, 2026年, 1-2頁.

2.2 域外立法的陷阱：美國《雲端法案》與《外國情報監視法》第702條司法管轄範圍的真相

歐盟成員國長期以來一直相信，只要將資料伺服器設在自國領土內，資訊就會安全無虞。亞馬遜、微軟與 Google 等美系企業，也在法蘭克福、巴黎或都柏林興建資料中心，並將這種信念作為廣告文案。然而，伺服器座落於歐洲土地上的事實，與該伺服器內部的資訊是否位於美國法律觸及不到之處，完全是兩回事。因為美國國會制定的兩部法律——《雲端法案》與《外國情報監視法》第702條，運作基準並非國界，而是公司的隸屬關係。

要理解這兩部法律為何如今讓歐洲的採購主管神經緊繃，首先必須了解《雲端法案》誕生的背景。2013年12月，美國聯邦執法機關因涉毒調查，向微軟發出令狀，要求交出某位使用者的電子郵件帳戶資訊。問題在於，該帳戶的資料儲存於愛爾蘭都柏林的伺服器中。微軟提出訴訟，主張美國令狀的效力不及於美國領土之外的資料；2016年，紐約聯邦上訴法院判決微軟勝訴。

在美國司法部不服此判決並將案件上訴至聯邦最高法院期間，美國國會於2018年3月23日通過了《雲端法案》。由於新法改變了這場爭訟本身的法律依據，最高法院認定無須進一步審理，遂終結了訴訟。《雲端法案》正是美國政府在官司即將敗訴之際，透過立法收拾殘局而誕生的法律。

這部法律的核心極為簡單：它不問資料儲存於哪一個國家，只問管理該資料的公司是否處於美國的司法管轄範圍之內。在法律用語中，這以「占有、保管、控制」三項標準來表達。無論是總部設於美國的公司，抑或由美國公司掌控股權與經營權的海外子公司，只要是該公司所占有、保管或控制的資訊，無論其儲存的物理位置為何，都必須依據美國法院的令狀或命令予以提交。

在此處，有必要將《雲端法案》實際上促成的效果，與大眾常見的誤解區隔開來。《雲端法案》所賦予的能力非常明確：處於美國司法管轄範圍內的通訊服務提供者或遠端運算服務提供者，只要是其所占有、保管或控制的資訊，無論部位於世界哪一個國家的伺服器上，都有法律義務配合美國政府的合法要求予以提交。相對地，《雲端法案》並不自動意味著許多事。首先，這部法律並不代表美國政府已經掌握了所有的資料。

政府依然必須在各個具體個案中，經過法院令狀或檢察官傳票等正式的法律程序。其次，這也不意味著所有的要求都會自動獲得貫徹。《雲端法案》僅針對與美國政府正式簽署相互執行協定的外國政府國民，為企業留出了一條向法院提出抗辯的狹窄管道。自2022年以來，簽署此類協定的國家僅有英國與澳洲兩國，歐盟至今尚未與美國簽署此類協定。因此，關於歐洲公民的資訊，甚至連這種例外性質的抗辯程序都不適用。

即使是已簽署協定的英國，這條管道也並不寬敞。請求對象必須非美國國籍者且未居住於美國，並且公司必須證明交付資訊的行為確實與英國法律相衝突，法院才會採納抗辯。而在像歐

盟這樣根本沒有簽署協定的情況下，連這種有限的管道都不複存在。第三，這部法律的涵蓋範圍取決於公司的國籍與控制結構，而非伺服器的物理位置。若是與美國毫無股權關係或經營關係的純粹歐洲公司，就不會成為《雲端法案》的適用對象。

若順著一個具體的流程來審視這種結構，便很容易理解。假設法國某個行政部門與美國公司的歐洲子公司簽訂合約，並在合約中納入了「資料必須保存在法國領土內」的條款。這份合約是法國政府與歐洲子公司之間的約定。然而，若美國檢方想要獲取該資料，檢方發出令狀的對象並非位於法國的子公司，而是位於美國的母公司。母公司作為掌控子公司股權與經營權的主體，在法律上被視為處於占有、保管、控制該資料的地位。

當母公司指示子公司提交資料時，子公司無論與法國政府簽訂了何種合約，都別無選擇只能遵從該指示。法國政府僅為合約的相對人，無權干預此一內部指示過程。即便資料一次也沒有離開過法國領土，這一程序依然會照常進行。資料僅憑留存在歐洲這一條件，法律風險並不會因此消失，原因即在於此。決定風險的並非伺服器座落的位置，而是管理該伺服器的公司國籍與控制結構。

在此之上，還疊加了另外一層因素。歐盟《一般資料保護規則》第48條規定，即便外國法院或行政機關要求傳輸個人資料，除非該要求是基於歐盟或成員國簽署的國際協定，否則不得在歐盟境內直接獲得承認或執行。然而，如前所述，美國與歐盟之間並不存在依據《雲端法案》簽署的相互執行協定。最終，收到美國令狀的公司便陷入了兩部互相對立的法律夾縫之中。

若遵從美國令狀，就會在缺乏歐盟法律所要求的國際協定依據下交付資訊；若拒絕令狀，則可能在美國法庭上面臨藐視法庭的法律責任。這種衝突並非紙上談兵的爭議，而是美系雲端企業每次與歐洲客戶簽訂合約時，實際面臨的結構性困境。

義大利的案例展現了這種困境究竟根深蒂固至何種地步。義大利政府在建立用於公共行政的本國戰略雲端「國家戰略雲端」（Polo Strategico Nazionale）時，設計為將資料僅保留在義大利領土內，連加密金鑰也由本國機構直接管理。然而，實際驅動該戰略雲端的底層技術，卻是微軟 Azure 與 Google Cloud 等美系超大規模雲端業者。義大利當局即便握有金鑰，也無法完全消除「用來鎖門的鎖具本身是由美國公司設計並提供」這一根本局限。

即便築起了資料位置與加密金鑰這雙重防線，軟體源頭技術的國籍這一第三層結構，依然留在美國。

這一實質真相並非抽象的法律條文，而是透過實際證言得到了證實。2025年7月17日，微軟的法務主管出席法國參議院聽證會，在宣誓後作證。他承認，即便使用者資料實體儲存於巴黎，一旦美國聯邦執法機關依據《雲端法案》要求提交資訊，公司也別無選擇，只能在未獲得法國政府批准的情況下將該資訊交付出去。

2025年7月22日，美國財經雜誌《富比士》報導這項證詞後，全歐洲負責採購的公務員終於透過書面文件確認了一個事實：僅憑將伺服器設在自國領土內的政策，並無法擺脫美國法律的管轄

射程。

與《雲端法案》形成雙軌威脅的另一大隱憂，是《外國情報監視法》第702條。該條款包含於2008年通過的《外國情報監視法》修正案中，允許美國國家安全局等情報機構在未針對個別對象取得法院搜索票的情況下，即可收集位於美國領土外之外國人的通訊紀錄與網路資料。若說《雲端法案》是偵查機關依據個別需求發動的執法工具，第702條則是情報機構以海外情報收集為名廣泛運用的監視權限。由於該條款設有有效期限，屬於限時法，因此美國國會每隔數年就必須重新審議並加以延長。

2024年4月，美國國會透過《情報改革與美國安全法》再次延長第702條，將其效力維持至2026年4月。此後國會又將期限進一步延至6月12日，但由於新的延長法案最終未能在該期限前通過，法律條文本身於2026年6月12日子夜正式失效。然而，美國外國情報監視法院已於2026年3月核准了一年期的監視認證，制度設計使其在法律失效後依然維持效力，因此實際的監視權限將持續運作至2027年3月。

法律條文的存廢與實際監視的持續與否如此背道而馳，這項事實本身就揭示了單憑一部法律要控制此權限是何等困難。多份報導曾指出，這套監視網不僅涵蓋普通市民，連盟國將領與高階外交官的電子郵件傳輸路徑亦被納入其中。至於第702條在現實中究竟如何運作，則在2013年透過前美國情報人員愛德華·史諾登的揭露而具體公之於世。

根據當時公開的文件，美國國家安全局以該條款為依據，運作著名為「稜鏡」（PRISM）的資料收集系統，直接從Google、微軟、雅虎等美國公司的伺服器調取外國用戶的資料。這起揭露事件成為歐洲各國不再將第702條視為紙上條文，而是將其視為實行中的監視基礎設施的契機。

這套監視結構首次在歐洲法庭發生正面衝突的事件，正是「施雷姆斯案判決」。2020年7月16日，歐盟法院在奧地利公民馬克西米利安·施雷姆斯提起的訴訟中，認定美國的監視體系嚴重侵害歐盟公民的個人資料自我決定權，進而宣告美國與歐盟之間的個人資料傳輸協定《隱私盾協定》無效。合議庭所指摘的核心問題，無非就是像第702條這類美國免搜索票的授權監視機制。

該判決的核心在於：無論歐洲企業在合約中訂定多麼嚴密的個人資料保護條款，只要該資訊經過美國公司的通訊網路，就無法透過合約阻擋美國情報機構自身的監視權限。歐盟委員會在2026年6月3日提出的《雲端與人工智慧發展法案》影響評估報告中，亦明確將《雲端法案》與第702條這兩者指為歐洲數位領土所面臨的結構性安全缺陷。

此問題並未停留在法律條文的解釋層面，而是轉化為改變實際採購政策的驅動力。德國巴登-符騰堡邦內政部對基於微軟軟體的公共雲端計畫「Delos Cloud」的實際運作條件進行了精密分析。分析結果相當明確：雖然資料中心本身獲得德國聯邦資訊安全局的認證並於德國領土內運作，但運行於其上的應用軟體設計與控制權，依然掌握在美國微軟公司手中。

邦內政部得出結論：只要應用層的控制權仍留在美國公司手中，就無法排除美國安全當局指示軟體供應商在用戶不知情的情況下植入資料外洩管道的可能性。資料在物理上位於德國境內這

一事實，並無法化解此一風險。

類似的疑慮在荷蘭演變成政府的正式決策。美國綜合資訊科技企業勤達睿（Kyndryl）於2025年11月宣布將收購荷蘭公司Solvinity。Solvinity是負責營運荷蘭約1,650萬名公民所使用的電子身分證系統「DigiD」基礎設施的公司。荷蘭國會眾議院隨後不斷提出疑慮，擔憂這起收購案可能讓美國司法管轄權有機可乘，進而獲取本國公民的敏感身分資訊，荷蘭政府遂啟動阻止收購的程序。

荷蘭經濟部政務次官阿爾茨於2026年5月26日以維護公共利益為由，正式宣布否決勤達睿對Solvinity的收購案。政府提出的理由非常明確：美國法律在理論上允許美國當局調取由美國公司所擁有的海外子公司伺服器中所儲存的資訊。這是自2020年成立以來，荷蘭投資審查局首次阻止美國企業的收購案。美國智庫策略與國際研究中心（CSIS）評估，這項決定將成為衡量歐洲多國未來投資審查基準如何轉變的試金石。

在英國，無論物理位置為何，合約本身即構成了將國家機密交付給美國公司的形式，使問題顯露無遺。美國資料分析企業帕蘭提爾（Palantir）與英國核武器研究機構「核武器機構」（AWE）簽訂了一份價值1,500萬英鎊的雲端支援合約。據調查媒體《The Nerve》於2026年1月報導，該合約並未登錄於政府的官方公開採購網站上，且英國國防部對該合約的存在既不承認亦不否認。

該報導統計，帕蘭提爾與英國政府簽署的合約總額高達6億7,000萬英鎊，而與核武器機構的合約則是其中未出現在公開名單上的已知規模。英國下議院科技委員會指出，當前將國家執法網絡與醫療數據仰賴美國公司的結構，是採購體系中的嚴重漏洞。涉核資訊的合約被排除於公開採購名單之外這一事實，再次證實了即便在物理國境內簽署合約，亦不意味著資訊控制權就會留在自國手中。

在德國，雖然也發生了與帕蘭提爾相關的另一起法律衝突，但必須區分的是，該事件的問題出在德國憲法，而非《雲端法案》或第702條。德國聯邦憲法法院於2023年2月16日裁定，警察運用軟體對無犯罪嫌疑的公民進行預測性分析屬於違憲。被判違憲的「HessenDATA」系統，正是基於帕蘭提爾的 Gotham 平台打造的治安軟體。該判決所質疑的並非美國法律的域外適用，而是德國《基本法》所保障的公民自我決定權。

這兩個問題雖然成因不同，但最終都指向了同一個結論。將國家治安資訊託付給美國公司軟體的架構，無論是出於美國法律還是本國憲法，都可能同時從多個方向遭到動搖。

事實證明，美國的境外司法管轄權不僅限於要求調取資訊，更能被用作制裁的工具。美國財政部外國資產管制局於2025年8月20日，對參與簽發以色列總理納坦雅胡逮捕令的國際刑事法院法官實施了制裁。法國籍法官尼古拉·吉尤也被列入制裁對象。此後他向媒體表示，自己的銀行卡支付與亞馬遜服務存取權限均遭切斷。另有報導稱，同獲制裁的其他國際刑事法院相關人員的電子郵件帳戶遭到微軟停權，但微軟方面對此予以否認。

這起事件雖然是基於與《雲端法案》或第702條不同的制裁法規，但卻展現了同出一轍的風險。依賴美國公司提供支付、通訊與雲端服務的個人及機構，僅憑美國行政部門的一紙決定，就可能瞬間失去對日常服務的所有存取權限。

法國更是直接將此問題明文寫入認證標準的條文之中。法國國家資訊系統安全局在修訂針對受信任雲端業者頒發的 SecNumCloud 認證標準時，明確指出僅將資料留存於歐洲境內的條件並不足夠。2025年修訂的 SecNumCloud 3.2 版本，除了要求申請認證的業者其總部所在地與資料中心必須位於歐盟境內之外，還新增了一項要件：公司的資本與表決權結構必須完全獨立於像《雲端法案》這類具有域外效力的第三國法律。

這意味著，業者必須具備即使第三國未透過國際司法協助程序而逕行下達資料公開命令、該命令也無法發揮作用的結構，方能獲得認證。法國主管機關在認證標準條文裡實質點名《雲端法案》的事實，顯示出歐洲的政策制定者已將此問題定性為無法單憑合約中的信任條款解決、而必須從公司的所有權結構層面切入處理的課題。

將這些案例綜合來看，可以得出一個明確的結論。將資料保留在歐洲領土境內的政策固然是必要的措施，但單憑這一點並不足夠。若要切實降低風險，處理資訊的公司本身必須脫離美國的所有權、控制權以及軟體設計權限。因為伺服器的位置不過是地圖上的座標，而實際上存取該座標內資訊的權限，取決於公司總部隸屬於哪個國家的法律管轄。這正是歐洲各國政府將審查範圍從實體資料主權擴展至公司治理結構與軟體源頭技術的原因所在。

歐盟執委會在雲端與人工智慧開發法案的影響評估報告中，將此一區分轉化為政策語言。報告將資料的實體儲存位置、加密金鑰的管理主體，以及設計與支援軟體的公司所有權結構，劃分為三個不同的層面進行審視。法國的 SecNumCloud 認證著手處置公司的資本結構，義大利的戰略雲端即便掌握了加密金鑰也無法宣告完全獨立，這些都是以各自的方式證明了一點：唯有這三個層面緊密結合、同時具備，實質的防護才能真正成立。

依據及參考文獻

1. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943 (Public Law 115-141), 2018年3月23日. 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), 2008年.

3. U.S. Congress, Reforming Intelligence and Securing America Act (RISAA), 2024年4月20日. https://www.congress.gov/crs-product/R48592

4. Electronic Frontier Foundation, 'Victory! 702 has Expired!', EFF Deeplinks, 2026年6月. 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, 2020年7月16日判決.

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), 美國聯邦最高法院. 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, 2025年7月22日. 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, 2026年6月3日. 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, 2024年. 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, 2026年5月26日. 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, 2026年6月. 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, 2026年1月. https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley

16. Bundesverfassungsgericht, 黑森數據預測警政程式相關判決, 2023年2月16日.

17. Irish Times, "It's surreal': US sanctions lock International Criminal Court judge out of daily life', Irish Times, 2025年12月12日. 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, 2026年. 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, 2025年. 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, 2013年6月6日.

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

2.3 「實體隔離（Air-Gap）」與自主架構：超越合約條款的技術隔離

微軟的法務負責人在2025年7月出席法國參議院聽證會時，在具結後宣誓證言。他表示，即使是儲存在巴黎的使用者資料，只要美國聯邦調查機構依據《雲端法案》（CLOUD Act）要求提交情報，微軟也只能在未獲法國政府批准的情況下交付資料。這項證詞向歐洲的行政官員清楚揭露了一個事實：僅憑將資料留存於本國領土內，以及在合約中填滿安全條款，並不足以擺脫美國司法管轄權延伸的範圍。

合約本質上是交易雙方將同意遵守的承諾留存為書面文件。歐洲各國政府在與美國雲端企業簽訂合約時，也一直加入不得將資料轉移至境外、未經歐洲法院命令不得交付情報等條款。然而，這類條款唯有在合約相對人企業能夠自由履行該承諾的情況下才能發揮作用。只要該企業仍受美國法律管轄，一旦美國政府以本國法律為依據下令提交情報，企業就必須在合約承諾與本國法律之間做出抉擇，而在絕大多數情況下，企業只能選擇遵守本國法律。

當對手企業被迫在本國政府的命令與合約上的承諾之間二選一時，合約上的文字便不再能成為保護傘。

這個事實瓦解了歐洲許多國家長期以來所依賴的一道安全機制。歐盟的個人資料保護規定早就要求將資料儲存於境內，許多公共機構也一直認為只要伺服器位於本國國境之內，資訊就是安全的。這種要求被稱為「資料在地化」。然而，資料在地化僅規定了資訊物理上位於哪一個國家，對於處理該資訊的軟體由誰設計、由誰掌握遠端存取的權限，則並未作出規範。伺服器的位置與系統的控制權，是截然不同的兩回事。

德國巴登-符騰堡邦內政部的分析具體揭露了這種差異。邦政府評估的 Delos Cloud（德洛斯雲端）專案，雖然設計為將資料實體存放於德國領土內的伺服器上，但實際運行該雲端的應用程式設計與更新權限，依然掌握在美國微軟總部手中。邦內政部以此為依據得出結論：即便資料位於德國土地上，只要系統控制權仍留在美國企業手中，就一步也未能擺脫《雲端法案》的搜查射程範圍。

問題不在於資料儲存在何處，而在於處理該資料的軟體由誰設計、由誰發布更新指令。

法國國內安全總局（DGSI）選擇「ArgonOS」作為其情報系統，以不同的方式回應了這兩個案例所暴露的問題。開發 ArgonOS 的 ChapsVision 是一間股份全數由歐洲股東持有的企業。該系統僅在與外部有線網路完全斷絕的實體隔離（Air-Gap）環境，或外部連線遭封鎖的主權雲端伺服器上運行。若擁有系統的公司沒有美國法人，且系統所在的網路不存在通往外部的管道，那麼即使美國司法機構簽發搜索票，也不存在執行該搜索票的管道本身。

這是一種並非依靠合約上的承諾，而是透過網路架構與所有權結構來實現隔離的方式。

這種隔離還包含超越保護資料本身的一項機制。ArgonOS 在處理數萬筆異質結構化與非結構化資料時，設計為由系統自主管理鎖定該資料的金鑰生命週期。即使資料經過加密，若該金鑰由外部企業管理，掌握金鑰的一方便能隨時開啟鎖頭。將金鑰管理與外部存取完全隔離，意味著不僅將資料內容，連同閱讀該資料的權限本身，都封鎖於本國境內。

唯有同時掌握伺服器位置與解密權限，隔離才能真正發揮作用。

「實體隔離（Air-Gap）」一詞字面上的意思是讓電腦網路與外部網際網路之間保持物理上的空白隔閡。由於沒有連接電纜，因此無法從遠端下達封鎖連線指令或強制停止系統。2026年6月發生的 Fable 5 封鎖事件正是瞄準了這個痛點。Anthropic 的模型透過網際網路提供服務，僅憑美國商務部的一紙命令，海外連線在數小時內即遭全面中斷。依賴外部網路的服務，無論合約多麼嚴密，在供應商總部所在國家的行政命令面前皆顯得無能為力。

相反地，若系統本身不存在任何與外部相連的管道，就不存在傳遞此類命令的物理路徑。

然而，擁有實體隔離架構並不意味著安全立刻大功告成。法國內政部表示，國內安全總局將整體實戰情報活動轉移至 ArgonOS 需要18至24個月。數十年來習慣了 Palantir 操作介面的特務員必須重新適應新系統，加上過去累積資料的儲存標準本身是針對美國系統設計，因此在轉移過程中仍存在資訊遺漏或格式不吻合的風險。法國國家行政部門為了填補這一空白，承諾在2027年前設立新舊體系並行運作的過渡期。

從決定轉移至隔離架構，到該架構真正完全運作之間存在著數年的時間差，而在這數年內同時維持兩種不同體系的負擔，便完全落在了情報機構肩上。

在這段時間差內所付出的代價並不局限於轉移期間。與外部網路斷絕的系統，也會同步切斷大型雲端企業所提供的即時更新與威脅情報共享服務。運作如 ArgonOS 這類自主系統的機構，必須依靠自身人力承擔安全補丁與功能改善作業，這也意味著選擇放棄美國大型雲端企業全球資料中心網路自動提供的規模經濟。

在完全沒有外部連線管道的環境中，連軟體更新都無法透過網際網路自動發布來處理，多半必須將更新檔案存入通過驗證的儲存裝置，經由實體帶入的方式進行。這種程序比網際網路更新更為緩慢，且每次都需配備專門的驗證人員來確認更新內容。這正是歐洲政策制定者選擇隔離卻未將其捧為萬靈丹的原因。隔離雖能防範外國政府單方面命令導致系統停擺的威脅，但代價是本國必須獨自承擔日常維護與保養的負擔。

區分實體隔離能夠解決與無法解決之問題的基準，也在於該系統究竟需要多少運算資源。像 ArgonOS 這樣負責單一機構情報分析的系統，即使採用相對有限規模的伺服器，也能在完全隔離的環境中運行。然而，像 Fable 5 這樣常態性需要龐大運算的大型人工智慧模型，情況則截然不同。若要讓這類模型在自國領土內、與外部斷開連結的狀態下進行訓練與運作，將需要單一機構無法獨自承擔的大規模資料中心、電力與半導體。

這正是 Fable 5 封鎖事件留給歐洲的課題，之所以超越個別系統的實體隔離，擴大為建構大陸規模運算基礎設施問題的原因。

瑞士與荷蘭的應對方式顯示，通往隔離的途徑並非只有一條。瑞士聯邦機構在 2018 年至 2025 年間，至少九度拒絕 Palantir 的投標方案，從一開始就未引進該公司的系統。與拆除已導入系統並遷移至新架構的法國或德國不同，瑞士並未經歷「轉移」這道昂貴的過程。荷蘭國防部雖在 2026 年 6 月向議會提交了會在兩年內取代 Palantir 的路線圖，但路線圖目前仍只是計畫，舊系統真正關閉、新系統全面運作的時間點在此之後。

從一開始就不建立依賴關係的選擇，與擺脫已經形成的依賴關係的選擇，即便朝向相同的目的地，所付出的代價卻截然不同。

完成了隔離的狀態也並非永久固定。當負責供應荷蘭行政網路核心軟體的在地企業 Solvinity 宣布將由美資企業 Kyndryl 收購時，荷蘭眾議院對管理本國 1650 萬市民資訊的基礎設施所有權可能在一夜之間轉移給美國企業的事實表達了極大疑慮。即使今天是歐洲企業持有的系統，若該企業明天被外國資本收購，以所有權結構為條件的隔離就會隨之崩解。

這正是為什麼證明隔離的程序不能僅止於導入時的一次性審查，而必須延伸為持續確認所有權與控制權結構變動的程序。

隔離架構所產生的摩擦，在跨國軍事合作中也顯露無遺。在北大西洋公約組織安全認證委員會於 2026 年 6 月 22 日認證 Palantir 的 Maven 智慧系統可用於全武器作戰的情況下，NATO 最高司令官們批評個別會員國在治安與行政領域採取的擺脫 Palantir 措施，是削弱軍事戰場效率的決定。將國內治安情報網遷移至與外部斷開連結的 ArgonOS 之選擇，與同盟軍共享的目標情報網依然在 Palantir 軟體上運作的現實，在同一個國家內部發生衝突。

即使一國的情報機構在自國領域內完成了隔離，也無法將該國所屬的整個同盟情報網一併隔離。隔離的邊界究竟要劃在哪裡，既是技術問題，也是決定如何維持同盟關係的政治選擇。

在政治宣示與架構完成之間，同樣存在著縫隙。在勒科爾紐部長宣布轉用 ArgonOS 之後，Palantir 公司依然表示其與國內安全總局簽訂的既有合約在法律上仍舊有效。政府的宣布、採購程序的轉換、合約的實際終止，以及系統的完全替換，並非在同一天一口氣發生的事件。從發布政治宣示的時間點到舊系統實際關閉的時間點之間，仍留有談判與執行的獨立過程，在此期間，舊合約在文書上依然可能具有法律效力。

宣布終止合約本身並未完成隔離，完成的證據不在於聲明稿，而在於實際停止運作的舊系統與實際開始運行的新系統。

法國與德國的這項決定，值得注意的是它們並未等待歐盟層級的法律制定，而是由各國政府率先做出決定。國內安全總局轉用 ArgonOS 與聯邦憲法保衛局做出相同選擇，都是透過個別國家的採購程序完成的。這顯示出，即使在合約與採購這類熟悉的程序中，只要將供應企業的所有

權結構與網路構成列為條件要求，便能創造出實質的隔離。在法律跟進之前，個別國家已先行改變了架構本身，而歐盟的下一項課題，就是將這些個別案例轉化為共通的採購標準。

歐盟委員會正試圖將這項隔離原則轉化為採購規定，而非放任由個別企業自行選擇。委員會於 2026 年 6 月提出的《雲端與 AI 發展法案》提案，目前仍是尚待歐洲議會與理事會審議的法案草案，並非已制定的法律。儘管如此，該提案已確立了方向，擬定了針對供應企業的所有權結構、董事會國籍乃至外部對原始碼的存取權進行審查的分級體系，要求以系統本身的設計而非合約上的承諾來證明隔離。

在最高等級中，目前正在討論要求達到在系統設計與原始碼維護的全過程中，絕不允許外國資本有絲毫干涉的隔離水準草案。

要讓這套審查體系具有意義，證明隔離的程序本身就不能僅止於供應企業的自主申報。法國已在運行的獨自認證規範 SecNumCloud，採用的是由政府指定的審查機構定期審計軟體設計圖與原始碼的方式。不能僅憑貼上了實體隔離或主權雲端的標籤，就認定隔離已經完成。唯有當外部審計員能夠親自確認網路架構圖、股權登記簿與原始碼儲存庫時，該標籤才具備實體。

《雲端與 AI 發展法案》提案中亦包含要求具備歐盟網路安全局營運認證體系中最高等級資格的方案，因而被設計為由國家層級認證與聯盟層級認證共同確認隔離的雙重結構。

合約與架構並非相互替代的關係，而是必須共同運作的關係。合約作為規定採購價格、服務品質與責任歸屬的文件，至今仍有其必要。然而，在如國家安全這般必須徹底切斷外國政府介入可能性的領域中，若合約所承諾的保護缺乏系統的實體結構與所有權結構作為後盾，該承諾在危機時刻便無法獲得恪守。

合約條款只有在對方有意願遵守承諾時才能發揮作用。美國的《雲端法案》與《外國情報監視法》第 702 條已顯示出國家掌握著能撤回該意願的權限，而 Fable 5 存取封鎖事件則證明了該權限即使面對同盟國亦能實際行使。歐洲的情報機構與行政部門之所以轉向實體隔離與所有權結構隔離，正是因為親身經歷並體會到合約書所承諾的保護與網路設計實際創造的保護之間存在著落差。

填補這一差距的工作並非單憑一條法律條文就能完成，只有在歷經數年的移植、自主維護以及獨立審計這三項條件同時具備時，才能宣告完成。

根據與參考文獻

1. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026年6月17日, 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, 2025年7月22日, https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

3. 作者不詳, '確認並整理歐洲脱離Palantir趨勢至原始來源', 2026年.

4. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, 2026年6月16日.

5. Loïc Duval, 'La DGSI remplace Palantir par ChapsVision', InformatiqueNews, 2026年6月18日.

6. 作者不詳, 'La DGSI prépare la sortie progressive de Palantir au profit de ChapsVision', Solutions Numériques, 2026年6月17日.

7. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026年, 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), 2026年7月7日.

9. 無出處（補充一般知識）。(→ 補充說明數據在地化與技術隔離的概念差異，以及氣隙系統因與外部雲端的即時更新及規模經濟隔絕而須自行承擔維護負擔的一般技術原理。)

3.1 國內情報領域與軍事聯盟領域的差異

2026年6月16日，法國總理塞巴斯蒂安·勒科爾尼（Sébastien Lecornu）宣布，將對內安全總局（DGSI）一直採用的美國帕蘭泰爾（Palantir）軟體，轉移至由法國企業 ChapsVision 開發的 ArgonOS。同日《世界報》（Le Monde）報導，帕蘭泰爾方面主張其與政府簽訂的合約依然有效。宣布消息、終止合約與實際替換系統，是在不同時間點進行的獨立程序。6月16日的新聞僅是宣布啟動轉向，並非確認系統已完成向 ArgonOS 的轉移。

德國聯邦憲法保衛局（BfV）也採取了類似的做法。多家德國媒體報導，2026年5月，BfV 決定引進 ChapsVision 的 ArgonOS，以取代美國的監視軟體。荷蘭國防部於2026年6月提出計畫，打算在未來兩年內徹底淘汰帕蘭泰爾軟體。據悉，瑞士聯邦機構在2018年至2025年期間，至少九次拒絕了帕蘭泰爾提出的情報招標案。瑞士的這些拒絕並非單一政府倉促作出的決定，而是跨越多年、重複進行的採購裁量結果。

西班牙也出現了相同的趨勢。內政部長費爾南多·格蘭德-馬爾拉斯卡（Fernando Grande-Marlaska）中止了國民警衛隊（Guardia Civil）與帕蘭泰爾合作進行的數據分析專案。西班牙軍事情報中心於2023年簽署的1,650萬歐元合約，到期後未獲續約。軍方高層雖要求維持合約，但未獲採納。西班牙政府改為透過該國技術轉型公司投入7.2億歐元，建置自主的人工智慧數據中心。比利時政府則宣布，將在2029年前投入10億歐元，自行建設軍用數據儲存設施。

在英國，衝突表現得更加顯著。英國下議院科學、創新暨科技委員會發表報告，指責將公共數據分析網絡交予美國私營企業的結構是安全上的漏洞。針對英國國家醫療服務體系（NHS）與帕蘭泰爾簽署的3.3億英鎊合約，下議院議員要求終止合約。他們指出問題在於，即使支付了鉅額費用，政府也未能取得設計數據結構的本體論（Ontology）控制權。這意味著合約結束後，英國政府手中將不會留下任何技術資產。

下議院建議政府以2027年2月起生效的主權理由解約條款為依據，劃清與帕蘭泰爾的關係。在丹麥議會，在野黨也在2025年5月提出了擺脫對美國軟體依賴的動議。

這些決定 coffees都是在單一國家內部作出的。國內情報機構與國防部擁有自行管理本國警察紀錄與情報資料的權限。在該權限範圍內，終止合約並轉移至其他公司產品的程序也能相對快速地推進。這背後有法律上的原因。美國國會於2018年3月制定的《雲端法案》（CLOUD Act）規定，只要服務是由美國法人所控制經營，無論儲存資料的伺服器位於哪國，在美國執法機關提出正式請求時，都必須提供資料。

該條款實際應用於哪些案件、相關請求是否每次均依法處理，屬於須視個別案件而定的問題。然而僅憑該法案的存在，歐洲情報機構便將本國偵查資料存放在美國企業伺服器架構內的狀態視為一種負擔。

與此同時，多邊軍事聯盟的決定卻朝著相反的方向發展。北大西洋公約組織（NATO）旗下的通訊與情報局（NCIA）於2025年簽署合約，引進帕蘭泰爾的「瑪文智慧系統」（Maven Smart System）供盟軍作戰司令部使用。該合約從制定需求規格到簽署，僅歷時約6個月。一年多後的2026年6月，北約安全認證委員會確認了該系統具備完整的技術作戰能力。簽署採購合約的時間點與獲得完整作戰能力認證的時間點並非同一件事，兩者之間經過了漫長的驗證與測試階段。

出現這種差異的原因，在於這兩個領域所處理的業務結構本質上有所不同。單一國內情報機構所使用的系統，僅供該國國境之內、遵循該國法律的人員存取。法國對內安全總局調查員撰寫的案件紀錄在 ArgonOS 中以法文儲存，且必須經過法國檢察機關與法院的程序才能外流。相較之下，瑪文智慧系統從一開始就被設計為讓三十多個國家的軍人觀看同一畫面，並共享同一份目標清單。

美軍的阿內爾·戴維斯（Arnel David）上校表示，在該系統內開發的戰術應用程式已超過50個，且這些程式均遵循北約盟軍的通訊標準 STANAG 4774 與 4778。遵循標準意味著波蘭軍人輸入的坐標，挪威軍人能立即讀取，美軍飛行員也能根據該坐標設定航線。國內偵查紀錄是不跨越國界才安全，而聯合作戰的目標資訊則是必須跨越國界才有價值。這兩項業務的安全標準本身便指向相反的方向。

北約最高層人士將這種差異解釋為軍事必要性，而非政治選擇。北約盟軍轉型最高司令皮埃爾·范迪埃（Pierre Vandier）法國海軍大將承認，歐洲軍隊目前尚不具備可用於自動分析衛星影像及協調彈藥補給的自主軟體。他表示，在替代技術成熟之前，絕不能削弱聯盟的作戰執行能力。包括凱·羅爾施奈德（Kai Rohrschneider）司令在內的其他指揮官亦警告，若成員國各自使用不同系統，加密通訊網絡之間的連線可能會中斷。

他們的邏輯是，若單一國家為了維護情報主權而削弱整個聯盟的通訊體系，所造成的損失將更為巨大。

這項邏輯也面臨反駁。成員國在國安領域排斥帕蘭泰爾的原因，在於美國國內法賦予了美國執法機關存取美國企業伺服器的權限。若在國內情報網絡中嚴重看待這項疑慮，卻在北約指揮體系內不予採納，那麼劃分標準便非取決於資料的性質，而是取決於簽約對象為國內機構還是多國聯盟。

這種矛盾同樣體現在資本的流向上。根據德國網路媒體 netzpolitik.org 的報導，在歐洲各國政府與帕蘭泰爾保持距離之際，歐洲多國的銀行與資產管理公司購買帕蘭泰爾股票的規模反而有所增加。帕蘭泰爾在2026年第二季財報中宣布，營收較一年前增長了93%。在公共部門淡出帕蘭泰爾的同時，民間資本卻在同一時期向帕蘭泰爾進一步靠攏。

在此之前，德國聯邦憲法法院於 2023 年 2 月 16 日裁定，黑森邦警察基於 Palantir 的 Gotham 引擎所開發的自動數據分析系統「Hessendata」違憲。憲法法院認為，該系統自動整合個人資

料以篩選危險人物，缺乏充分的法律依據。這項判決甚至早於歐盟《人工智慧法案》的制定，率先展現了國內憲法秩序能夠獨立於國家安全例外之外，對國內治安用途的人工智慧系統加以管制的實例。

單一國家的憲法法院擁有為本國警察系統施加制動的力量。然而，在三十二個國家共同使用的同盟指揮體系中，卻沒有任何單一機構具備這樣的制動機制。國內情報領域的脫離與軍事同盟領域的擴大，其分歧點在於該領域是否存在能夠進行管制的權力主體。

根據與參考文獻

1. 法國參議院調查委員會, '歐盟(EU)主要國家脫Palantir動向與數位主權化分析報告', 法國政府官方門戶, 2026.

2. 約翰·亨利, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026年6月16日.

3. 記者未詳, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026年6月17日.

4. 佚名, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, 2026年5月26日.

5. IT-Daily 編輯部, 'Palantir: Bundesamt für Verfassungsschutz wählt ChapsVision', IT-Daily, 2026年5月.

6. 科林·巴克, 'Defensie wil binnen twee jaar af van Palantir-software', ICTMagazine, 2026年6月3日.

7. Egle˙Kristopaityte˙, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, 2026年7月2日.

8. Le Soir 編輯部, 'Palantir s'implante en Belgique: 28 questions à (se) poser', Le Soir, 2026年3月19日.

9. Novara Media 編輯部, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026.

10. 英國下議院科學技術委員會, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', UK Parliament, 2026.

11. 揚·埃貝爾, '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. 德國聯邦憲法法院, 'Decisions search - Judgment of 16 February 2023', 德國聯邦憲法法院, 2023年2月16日.

14. 作者未詳, '查證至原始來源整理之歐洲 Palantir 離場趨勢資料', 2026. (根據瑞士九次拒絕投標及丹麥在野黨提案)

15. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE 官方新聞稿, 2026年6月30日.

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 北約「Maven 智慧系統（MSS）」獲得完全作戰能力與互操作性的陷阱

美國國防部於2017年啟動了以人工智慧分析無人機與衛星影像來搜尋軍事目標的「Maven 計畫」（Project Maven）。帕蘭提爾（Palantir）以此計畫為跳板打造出商業版本，而這個商業版本正是北約所引進 Maven 智慧系統的根源。

北約通訊與情報機構（NCIA）於2025年與帕蘭提爾簽訂合約，以供盟軍作戰司令部使用該系統。從制定採購需求規格到簽署合約書的時刻為止，歷時約6個月。在此時間點，北約所取得的是使用該系統的權利與合約，並非可在所有軍事活動中隨時使用的認證。

完整的技術性作戰能力，即 FOC（Full Operational Capability）認證，則是在那之後過了一年多才核發。北約安全認證委員會於2026年6月22日確認，Maven 智慧系統已達到可在機密網絡中運作的水準。NCIA 代理營運總監巴爾特·范·梅爾特於6月26日向盟國司令部報告了這項認證結果。北約最高司令部（SHAPE）於6月30日正式宣布，該系統可在包含演習與實戰在內的所有軍事活動領域中不受限制地使用。

NCIA 總經理狄倫·布朗表示，對於能夠透過合作將這項能力轉交給聯軍戰鬥人員感到無比自豪。

ในสัญญาที่ลงนามในปี 2025 และการรับรองความสามารถในการปฏิบัติการอย่างสมบูรณ์ในปี 2026 มีช่วงเวลาทดสอบ ระบบนี้ผ่านการฝึกซ้อมที่ใกล้เคียงกับสถานการณ์จริงในการซ้อมรบหลายชาติ Steadfast Deterrence ที่สิ้นสุดลงในนอร์เวย์เมื่อวันที่ 13 พฤษภาคม พลตรี Ruprecht von Butler ผู้บัญชาการกองกำลังป้องกันประเทศเยอรมนี กล่าวว่าการฝึกครั้งนี้ได้ยืนยันความสามารถของระบบปัญญาประดิษฐ์ในการสร้างสถานการณ์จำลองการปฏิบัติการของศัตรูโดยอัตโนมัติ

Maven 智慧系統即時彙整並分析由軍事衛星、無人機與雷達傳送的資料。軍人透過觀看此螢幕，能大幅縮短選定打擊目標的時間。美軍阿內爾·戴維上校透露，在該系統內部開發的戰術應用程式已超過50個，而這些程式皆被設計為遵循聯軍通訊標準 STANAG 4774 與 4778。遵守此標準意味著成員國軍隊能夠與其他國家的軍隊安全地交換目標情報。

帕蘭提爾方面對資料所有權問題提出了明確立場。由帕蘭提爾派駐的費歐娜·布萊德利表示，Maven 智慧系統內的所有軟體與資料所有權皆歸北約盟邦所有，並說明自家具備不隨意加工客戶資料再轉售的原則。這番說明雖然回答了資料究竟屬於誰的問題，卻無法解答另一個問題——究竟由誰來設計處理該資料的程式結構。

修改系統核心程式碼與資料分類體系（即本體結構，ontology）的權限，依然掌握在帕蘭提爾的民間技術人員手中。北約成員國軍人所輸入的目標座標在合約上固然屬於盟邦資產，但整理與分類該座標的方式卻只能在帕蘭提爾所設定的框架內運作。若以圖書館作比喻，這種結構類

似於：書籍的所有權雖然屬於圖書館，但決定按何種順序分類上架的圖書館員座位上，坐著的依然是帕蘭提爾的員工。資料所有權與系統設計權並非同一種類的主權，北約所取得的是前者，而後者仍舊留存在帕蘭提爾內部。

該系統的效能在實際作戰中面臨考驗。美軍於2026年2月籌劃針對與伊朗有關聯的武裝組織進行空襲。軍方在發動空襲後的前24小時內運行 Maven 智慧系統，篩選出超過1,000處潛在打擊地點。親眼目睹此結果的聯軍指揮官對美國軟體的處理速度表達了信任。

同一時期，法國、德國與荷蘭則在其國內領域做出了截然相反的決定。法國於6月16日宣布將國內安全總局的軟體遷移至 Argon OS，德國聯邦憲法保衛局也在5月做出了相同決定。德國聯邦國防軍托馬斯·多姆海軍中將則在4月將帕蘭提爾排除於國防雲端專案的最終採購規格之外。當北約高層指揮體系向帕蘭提爾的系統越陷越深時，這些國家的國內情報與國防採購網絡卻正一步步遠離該公司。

這兩種方向的舉動在北約內部引發了摩擦。旺迪耶司令承認，歐洲軍隊在衛星影像分析或彈藥補給協調方面，目前尚不具備足以媲美帕蘭提爾的自主軟體。他表示，在替代技術成熟之前，絕不能削弱盟邦的作戰能力。德國的凱·羅爾施奈德司令則警告，若成員國各自使用本國開發的系統，恐將面臨加密通訊網絡之間中斷連結的風險。

對此，法國開始測試自家替代方案。法國國防部於2026年6月在波蘭舉行的採購演習中測試了「阿卡迪亞」（Arcadia）平台。阿卡迪亞是由法國國防企業泰雷茲（Thales）、賽峰（Safran）以及 Mistral AI 共同開發的戰場感知軟體。法國陸軍副參謀長帕特里克·居斯泰爾將軍指出，北約毫無疑義地接納外國系統的慣例威脅到了本國的情報安全。法德兩國元首於2026年7月17日簽署聯合聲明，宣布將建構歐洲自主的主權數位骨幹。

阿卡迪亞若要站穩腳跟至足以取代 Maven 智慧系統的地步，尚需時日。在此期間，北約指揮體系對互操作性的要求將持續施壓，促使成員國共享目標情報並統一通訊標準，而該壓力則會將採購拉向已經過驗證且符合標準的帕蘭提爾系統。國內情報機關固然可以在國境之內做出決定並終止合約，但由32個國家共同使用的指揮體系卻非單一國家所能擅自變更。這種差異正是北約內部互操作性持續壓倒國內控制權的原因所在。

依據及參考文獻

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', SHAPE 官方新聞稿, 2026年6月30日.

3. Tamara Rozouvan, 'Maven Smart System achieves full operating capability with NATO', Janes, 2026年7月1日.

4. 努萊·泰勒, 'NATO's 'Digital Lethality Branch' Breaks Records in Drive for Alliance-Wide Interoperability', AFCEA International, 2026年7月31日.

5. 費爾南多·卡斯楚·德·貝羅, 'Foreign software, Europe's War: How Maven and Palantir are already making decisions for Europe', DigitalShield, 2026年7月15日.

6. 維基百科(Wikipedia), 'Palantir', 2026年8月9日最後修訂.

7. 記者不詳, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026年8月3日.

8. Egle˙Kristˇopaityte˛, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, 2026年7月2日.

9. T.Wiegold, 'Cyber-Kommandeur der Bundeswehr lehnt Software von Palantir ab', Augen geradeaus!, 2026年4月28日.

10. Cybernews 編輯部, 'France and Germany to build an alternative to Palantir', Cybernews, 2026年7月20日.

11. 約翰·亨利, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026年6月16日.

12. 作者不詳, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, 2026年5月26日.

3.3 歐盟《人工智慧法案》（AI Act）國安例外條款與監管盲區

《人工智慧法案》（AI Act）是一部根據人工智慧系統對人類可能造成的風險大小，實施不同監管強度的法律。風險越高的系統，所承擔的透明度、風險評估以及人類監督義務就越沉重。該法案第2條規定，僅出於軍事、國防、國家安全目的而投放市場或使用的人工智慧系統，不適用本法。此項例外並不區分開發或運作該系統的主體是政府機構還是民間企業。前言（Recital）第24條闡明了其依據。

即國家安全在歐盟條約體系下屬於由成員國單獨負責的領域，而軍事與國防活動因其性質，係在歐盟共同外交與安全政策下接受另行規範。

這項例外條款並非談判過程中偶然留下的漏洞，而是成員國積極爭取所取得的結果。根據「未來世代中心」（Centre for Future Generations）2026年春季號報告，法國與義大利、瑞典一同主導了以國家安全為由擴大例外範圍的遊說活動。這些政府希望執法機關在公共場所使用人臉辨識攝影機或生物辨識監控工具時，無需通過布魯塞爾的風險評估程序。結果，國內治安機關的情報網絡與軍事同盟的目標識別系統，一同排除在《人工智慧法案》的適用範圍之外。

處於該監管盲區內的代表性系統，為國內治安用的 Gotham 系列軟體與北約的 Maven Smart System。《人工智慧法案》對其他高風險系統所要求的文件化義務、追蹤故障與偏見的程序，以及由人類審查最終決定的機制，依法皆不強制適用於這兩套系統。北約安全認證委員會於2026年6月向 Maven Smart System 發放完全作戰能力認證的程序，並未經過該法案的審查。

然而，此項豁免並不等於毫無監管。第2條的例外僅限於專門用於軍事、國防、國家安全目的的情形。即便由同一家公司開發的同一款軟體，若用於公共行政或民間治安等非軍事用途，仍受《人工智慧法案》規範。例外並非貼在特定企業或特定客戶身上的標籤，而是附屬於該人工智慧實際用途的條件。

《人工智慧法案》繞過的領域，也並非完全缺乏其他法律機制。德國聯邦憲法法院早在2023年2月16日，即《人工智慧法案》制定之前，便裁定黑森邦警察的自動資料分析系統 Hessendata 違憲。這項判決確立了一項原則：即便是以國家安全或治安為名義的人工智慧系統，在各國憲法秩序下仍須具備獨立的法律依據。《人工智慧法案》的國安例外僅代表該法規本身不予適用，並不意味著成員國的憲法、個人資料保護法規以及議會的監督權限會隨之消失。

在北約層面上，亦非完全處於無法可管的狀態。Maven Smart System 必須通過北約安全認證委員會批准的事實本身，即意味著在《人工智慧法案》繞過的領域，取而代之的是北約自身的認證程序。然而，此項認證程序僅係依據軍事標準確認系統能否安全運行，並非按照《人工智慧法案》所要求的偏見審查或對公民的透明度義務等標準所設計。改變的只是監督的主體與標準，監督本身並未消失。

只是隨著該項監督被納入國防機密之下，公民檢視其結果的管道相較於國內情報領域已大幅收窄。

歐洲議會於2026年1月表決通過一項技術主權決議案，旨在減少對少數美國科技企業的依賴。議員們引述的依據為：若資料過度集中於微軟（Microsoft）與亞馬遜（Amazon）等美國企業，僅憑美國政府的一項決定，便可能導致歐洲的服務陷入癱瘓。美國政府對歐洲此類監管動向表示反彈，並暗示可能採取貿易報復。

法國與德國領袖於2026年7月17日簽署聯合聲明，提倡建立歐洲自主的主權數位骨幹（sovereign digital backbone）。該聲明所指引的方向，在於實際完成如 Arcadia 等自主軟體的開發。《人工智慧法案》的國安例外，是承認歐洲無法單靠法規來阻止對美國技術之依賴的條款，而非解決該項依賴的條款。填補監管力量無法觸及的空白，任務落在了歐洲自行研發的替代技術肩上。

依據及參考文獻

1. Regulation (EU) 2024/1689, Artificial Intelligence Act, Article 2 and Recital 24, 2024年 12月 13日.

2. Centre for Future Generations, 「Enforcement spotlight - Spring 2026」, Centre for Future Generations, 2026年 春季號, 2-3頁.

3. 德國聯邦憲法法院, 'Decisions search - Judgment of 16 February 2023', 德國聯邦憲法法院, 2023年 2月 16日.

4. 法國參議院調查委員會, '歐盟(EU)主要國家脫(脫)Palantir動向與數位主權化分析報告', 法國政府官方門戶網站, 2026.

5. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE 官方新聞稿, 2026年 6月 30日.

6. 荷蘭國防部及歐洲技術委員會, '歐洲Palantir脫離趨勢追溯至原始來源之整理資料', 2026.

4.1 雲端與 AI 開發法（CADA）與資料中心加速區的規管創新

歐盟委員會於 2026 年 6 月 3 日正式提出《雲端與 AI 開發法》草案。英文名稱為 Cloud and AI Development Act，簡稱 CADA。文件編號為 COM(2026) 502。這一點必須先予釐清：CADA 目前仍非正式法律。這是歐盟委員會提請歐洲議會與歐盟理事會審議的規章草案，截至本書所探討的 2026 年 8 月 11 日為止，尚未獲得正式通過。

在歐盟，規章（Regulation）與指令（Directive）不同，無須經過成員國議會的個別立法即可直接生效，屬於效力較強的法律形式。正因如此，規章在獲確定通過前的審議程序也極為嚴謹。在普通立法程序中，歐洲議會與歐盟理事會須分別提出修正案並進行表決後，條文內容方得確定。在此過程中，目前提案文本中的條文與數據均可能有所變動。本章所說明的四階段主權保證層級、加速區以及解約權條款，全數皆為提案階段的藍圖，並非已經對成員國政府與企業具備約束力的規範。

區分兩者亦有助於避免混淆歐盟《人工智慧法》（AI Act, Regulation (EU) 2024/1689）與 CADA。《人工智慧法》已於 2024 年正式頒布並生效，該規章依據風險程度對人工智慧系統進行分類，並賦予相應義務。相對地，CADA 則是規範運行該人工智慧所需的基礎設施與採購程序之獨立提案，截至 2026 年 8 月尚未頒布。切不可僅因這兩部法律名稱中皆含有「人工智慧」字樣，便將二者的法律地位混為一談。

一者為已在施行中的規範，另一者則為尚待審議的提案。

CADA 是歐盟委員會持續推動的「人工智慧大陸行動計劃」之一部分。該計劃的目標可歸納為二：擴充歐洲境內資料中心的運算能力，以及保護該運算能力免受歐洲以外司法管轄權的干預。這兩大目標之所以被納入同一法案，背景源於歐洲雲端市場的結構。多份業界報告指出，亞馬遜（Amazon）、微軟（Microsoft）與 Google 這三家公司在歐洲雲端基礎設施服務市場中佔據絕對優勢的比重，而總部位於歐洲的企業所占份額則遠不及此。

科技政策媒體 Tech Policy Press 在 2026 年 6 月 15 日的報導中指出，這種過度傾斜會導致公共系統的命運置於外國司法權之下，形成安全漏洞。

在 CADA 出臺之前，歐洲也曾有過類似的嘗試。2019 年由法國與德國主導發起的 Gaia-X，是一項旨在建立歐洲企業可共同使用之資料基礎設施標準的民間主導計畫。然而，Gaia-X 僅為不具法律約束力的自願性協議體，隨著參與企業間的利益紛陳，普遍被認為未能達成最初預期的成效。CADA 與 Gaia-X 的不同之處在於，它並非自願性標準，而是企圖以具備法律約束力的規章直接推動採購市場本身。

然而，該規章若要真正具備效力，仍須通過歐洲議會與歐盟理事會的審議；就此而言，CADA 目前同樣尚處於宣示意志的階段。

對於一般讀者來說，這或許是個陌生的概念。政府、醫院或警察所使用的電腦系統，未必是在該國國境內的建築物中運行。若租用亞馬遜、微軟或 Google 等公司的雲端服務，實際的運算乃是在該公司於世界各地建立的大型伺服器園區中進行。業界將這種超大型伺服器園區稱為超大規模業者（Hyperscaler）。即使伺服器建築物在物理上位於歐洲土地上，只要擁有並營運該建築物的公司是美國法人，美國政府的法律要求仍可能延伸至其上的資料。

物理位置與法律控制權可能互異的這層落差，正是貫穿本章整體的核心論點。

此外，雲端產業中存在著一種被稱為「資料重力」（Data Gravity）的現象。一旦將大量資料轉移至特定公司的雲端，處理該資料的其他程式與服務若同樣置於同一雲端內，運行速度會更快且成本更低。這意味著隨著時間推移，資料以及處理該資料的應用程式，將會越來越深地綑綁於單一公司的生態系統之中。公共機構起初可能僅以租用儲存空間的形式簽訂合約，但往往不過數年，整體行政業務便陷入沒有該公司雲端即無法運作的困境，此類情形屢見不鮮。

這正是歐洲的政策制定者比起市場占有率數據、更為擔憂這種綑綁深度的原因所在。

前歐洲中央銀行總裁馬里奧·德拉吉（Mario Draghi）於 2024 年 9 月向歐盟提交的《競爭力報告》，常被引用為預先對此問題發出警告的文件。德拉吉報告建議，歐洲若要獨立開發人工智慧並營運服務，必須具備獲主權保障的運算處理能力。此項建議隨後反覆出現在歐盟委員會的各項政策文件之中。光是在歐洲境內設置伺服器絕非充分，還必須考量控制該伺服器之企業的國籍與股權結構——這種認知正是 CADA 提案的出發點。

歐盟委員會將這項資料中心擴建目標，與名為「人工智慧超級工廠」（AI Gigafactory）的獨立計畫綑綁推進。「人工智慧超級工廠」是指配備大規模圖形處理器（GPU）叢集的超大型運算設施，該概念最早於「人工智慧大陸行動計劃」中提出。該計畫背後的目標，不僅止於增加伺服器數量，更要在歐洲內部確保能夠從頭到尾完整訓練大型人工智慧模型的運算能力。迄今為止，歐洲的研究人員與企業若要訓練大型模型，皆必須租用美國雲端公司所提供的運算資源。

CADA 與人工智慧超級工廠，正是企圖改變這種租賃結構本身的嘗試。

值得一提的是，支撐此一目標的基礎設施已有部分投入運作。歐盟自 2018 年起便透過「歐洲高性能力計算聯合企業」（EuroHPC Joint Undertaking），與成員國共同營運超級電腦。將芬蘭的 LUMI 或西班牙的 MareNostrum 等既有超級電腦轉型為人工智慧訓練用運算資源的計畫，在 CADA 提出之前便已展開。

CADA 與人工智慧超級工廠的構想並非要完全取代這些既有資產，而是設計為在其基礎上進一步引進民間資本與成員國預算，以擴大規模。

歐盟委員會說明的 CADA 數字目標非常明確。那就是要在未來 5 到 7 年內，將歐盟的資料中心容量提升至三倍以上。目標是利用擴增後的容量，在 2035 年前滿足企業與公共行政的需求。這

一目標已載於歐盟委員會發布的提案文件本身。設定如此高目標的原因，在於供需之間的差距已經拉開。

歐洲議會於 2026 年 1 月 22 日通過的《歐洲技術主權與數位基礎設施》文件指出，全球電力消耗有相當大的一部分來自資料中心與電信設施，並預測歐洲資料中心的用電比重將在未來幾年內顯著增加。隨著人工智慧運算全面展開，這一比重還會進一步陡升。如果興建資料中心的速度趕不上需求，歐洲在人工智慧開發方面將難以擺脫向美國或中國租用雲端服務的處境。

問題在於興建資料中心這件事本身進度緩慢。每當成員國試圖建立新的公共行政資料儲存設施時，複雜的許可程序、土地管制與環境影響評估屢屢阻礙計畫推進。德國聯邦資訊安全局與國際律師事務所 Bird & Bird 於 2026 年 4 月 27 日聯合發布的報告指出，德國聯邦政府與各邦政府之間的行政程序不一致，從採購規格書階段就引發了延誤。這種延誤並非德國獨有的問題。

大規模雲端伺服器建置計畫因當地居民反對或環境審查延誤而遭縮減甚至取消的情況，在歐洲多個國家屢見不鮮。僅在某個地區選定資料中心用地、接入電力並取得許可，就需要耗費數年時間，而在此期間，運算需求的增長速度卻遠遠快於此。

CADA 提案以程序創新為核心主軸，旨在減少此類延誤。政治媒體《Politico》歐洲版於 2026 年 6 月 4 日報導指出，CADA 建議成員國政府將地理與電網條件優良的場址指定為「資料中心加速區」。律師事務所 Bird & Bird 整理的技術主權套案概要報告亦證實了該提案的意旨：在此類加速區內，許可程序將整合至單一窗口，並設定處理時限上限。如此一來，業者無需奔波於多個機關之間，而是能在單一窗口協調計畫的完整生命週期。該單一窗口試圖整合的程序相當多元。

該做法旨在將以往由不同政府機關分別管理的程序，例如電網連接批准、自來水與冷卻水供應許可、建築安全審查以及電信線路接入許可，統一由單一窗口進行協調。在此之前，業者必須依序逐一完成這些程序，只要其中一個階段發生延誤，後續的所有程序都會隨之順延。據報導，在此類加速區內，處理機密資料設施的許可審理時限最高限制為 18 個月。

考慮到以往興建單一大型設施所需的許可程序耗時數年並非罕見，這項上限可被視為從根本上重塑程序本身的訊號。

同一份報告指出，環境影響評估程序也針對加速區內的計畫朝簡化方向進行設計。這種簡化究竟是達到免除環境審查本身的程度，抑或僅是縮短審查期間，仍需等待該提案送交歐洲議會與歐盟理事會審議後方能具體化。目前階段要以確定條文下定論尚為時過早。然而，其方向性相當明確：若是與國家安全直接相關的基礎設施計畫，將賦予比一般地方政府許可程序更高的優先權。

據悉，將場址指定為加速區的權限主要歸屬於成員國政府。具體方式為地方政府或中央政府篩選出具備電網剩餘容量、通訊線路接入便利性及實體安全的場址並向歐盟委員會提出建議，再

由歐盟委員會進行審查並納入最終名單。外界評估，該程序借鑒了《晶片法案》現已實施的晶圓代工廠場址指定機制。

這一擴建目標亦與歐盟的氣候目標相互關聯。歐盟已透過《歐洲綠色政綱》確立了在 2050 年前實現碳中和的目標。在資料中心用電量持續增長的情況下，若要恪守此目標，勢必面臨新設設施須有相當大一部分採用再生能源運轉的壓力。CADA 將加速區的優惠措施與永續性標準相掛鉤，可被解讀為絕不為追求速度而犧牲氣候目標的訊號。

加速區構想同樣伴隨著風險。若缺乏驗證受惠計畫是否確實符合公益的機制，快速通過審查程序的優惠可能會演變成浪費稅金。在瑞典，政府曾於 2022 年以擴建本國技術基礎設施為由向資料中心企業提供租稅優惠，但隨後遭指責缺乏驗證該些企業是否確實履行再生能源使用計畫的機制。瑞典媒體 SecurityUser.com 於 2026 年 3 月回顧此問題時報導稱，北歐各國正重新設計數位主權基礎設施政策。

Bird & Bird 的報告說明，為了避免重蹈覆轍，CADA 提案包含了一項安全機制，要求獲得加速優惠的業者證明其符合永續性標準。這等於是在為了追求速度而簡化程序的同時，以要求驗證結果的新義務作為相應代價。

從財政規模來看，即可看出 CADA 並非單打獨鬥的法案。歐盟委員會於 2026 年 6 月 3 日一併公開的附屬文件（COM(2026) 555 final/2）估計，要完全落實《雲端與人工智慧開發法》及《下一代安全套案》，到 2036 年為止共需要高達 3,000 億歐元的投資。其中 2,000 億歐元將用於資料中心基礎設施擴建；該文件預測，另有 1,000 億歐元將分配給晶圓代工廠與人工智慧超級工廠（Gigafactory）的建置。

這項投資計畫並非僅針對《雲端與人工智慧開發法》單一法案。若說 2023 年生效的歐盟《晶片法案》著重於擴充半導體產能，CADA 的財政計畫則更接近於為運行在該半導體之上的資料中心與人工智慧基礎設施提供支援的後續計畫。產業分析報告 innobu 說明，這兩部法案綁定在一起，構成了歐洲的技術主權套案。不過，該數字僅為歐盟委員會的估算，實際執行預算仍須經過成員國與歐洲議會的預算協商方能確定。

歐盟各國領袖於 2025 年 11 月 18 日齊聚柏林並發表安全峰會共同聲明一事，被視為該財政計畫的政治背景。

這項基礎設施擴充所應對的威脅性質，與第二章探討的模型存取封鎖層次不同。Anthropic 暫停外國使用者存取 Fable 5 的事件，是發生在軟體層面的問題。僅憑美國政府的一道出口管制指令，特定模型的存取權限本身就被封鎖。相較之下，在未擁有資料中心的情況下產生的威脅則更為根本。若處於運算能力本身必須向他國企業租借的境地，就意味著被封鎖的不只是模型，連運行該模型的硬體也可能無法存取。CADA 所針對的，正是這種硬體層面的脆弱性。

綜合鴻鵠律師事務所（Bird & Bird）與 IT 媒體 ITWelt 的報導，CADA 提案同時提出了引導歐盟境內相當數量的私營企業在 2030 年前遷移至主權雲端服務的目標值。此外，還提及了一項構

想，即在大陸各地密布低延遲邊緣運算據點，從而在消費者服務領域也降低對美國大型平台的依賴。這些目標在最終法規中會保留為強制性義務，抑或放寬為建議性質，仍須視審議過程而定。

這種優先順序的指定付出了削弱在地社區發言權的代價。一旦資料中心被指定為國家層面的重要戰略事業，該用地居民在常規都市計畫程序中原本得以行使的異議提出與聽證會參與空間便可能遭到縮減。為了追求速度而縮減程序，同時也意味著壓低了原本存在於該程序中的在地居民聲音。CADA 最終將如何調和這項平衡，目前尚未定案。

在確保電力供應的方式上，各成員國之間的策略也出現分歧。核能發電比例較高的法國，正從政策層面強力推動在核電廠附近興建資料中心的方案。能將穩定的低碳電力直接供應給資料中心，被視為該策略的主要優勢。相反地，以再生能源為中心重組電網的國家，則必須另行解決how 讓太陽能與風力的間歇性配合資料中心24小時運作需求的問題。CADA的加速區指定標準中包含電網條件，看來也是考量到各國情況差異所作的設計。

加速區的劃定可能會集中於特定成員國，這一點也引發了討論。電網與電信基礎設施已相當完善的西歐及北歐部分地區極可能率先符合劃定要件，而基礎設施投資相對較慢的東歐與南歐部分地區則面臨落後的風險。歐盟區域均衡發展原則與資料中心加速推動這一速度邏輯該如何取得調和，亦是 CADA 在修訂最終條文過程中必須處理的課題。

CADA 所描繪的藍圖，歸根結底可歸結為一個問題。若歐洲無法自行建造用來儲存自身資料的實體空間，那麼討論在該空間上運行的軟體主權便顯得空洞。在實體資料中心這一基礎之上，還存在著另一個層次：究竟由誰來掌控該資料中心的標準。

根據及參考文獻

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, 2026年6月15日, https://www.techpolicy.press/does-europe-really-have-a-plan-for-tech-sovereignty-cada/

4. Mario Draghi, 「The Future of European Competitiveness」, European Commission, 2024年9月.

5. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', 歐洲議會公報, 2026年1月22日.

6. 德國聯邦資訊安全局, 「Digitale Souveränität bei IT-Vergaben: Zwischen politischem Anspruch und vergaberechtlicher Wirklichkeit」, Bird & Bird Insights, 2026年4月27日.

7. Tyler Weygold, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, 2026年6月4日, https://www.politico.eu/video/achieving-digital-sovereignty-a-golden-opportunity-for-the-eu-politico/

8. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, 2026年6月23日.

9. SecurityUser.com, 'Ny molnpolicy ska ge ökad digital suveränitet i offentlig förvaltning', SecurityUser.com, 2026年3月.

10. European Commission, COM(2026) 555 final/2, 歐盟公報, 2026年6月3日.

11. innobu, 'EU Tech Sovereignty 2026: Chips Act 2.0 and CAIDA', innobu Insights, 2026年6月.

12. Itwelt 編輯部, 'Best European cloud alternatives: Top 10 of 2026', Itwelt, 2026年2月.

4.2 CADA 的四階段主權保證層級（Sovereignty Assurance Levels）設計

CADA 提案設立的第二大支柱，不是資料中心這種物理外殼，而是判別在其中運行的軟體以及營運該軟體之企業國籍的標準。歐盟委員會將此標準劃分為四個階段。英文稱為主權保證層級（Sovereignty Assurance Level），簡稱為 SEAL。倫敦的安全政策研究機構布倫斯伯里情報安全研究所（BISI）於 2026 年 7 月 7 日發布的報告，將此四階段結構整理為 CADA 三大支柱之一，並解釋其設計目的在於阻斷美國《雲端法》（CLOUD Act）與《外國情報監視法》第 702 條對歐洲公共資料的影響力。

美國國會於 2018 年通過的《雲端法》，強制要求由美國法人掌握經營控制權的資通訊服務業者，無論資料儲存於哪一個國家，皆有義務向調查機關保存並提交資料。從法案內文與國會摘要中確認的該條款，亦可適用於設立在歐洲內部的美國企業子公司。這意味著，即使與歐洲企業簽訂合約、將伺服器設在歐洲領土內，並遵守歐洲的個人資料保護法，但若營運該伺服器之公司的母公司為美國法人，美國調查機關的要求便可能優先於合約內容。

據悉，歐盟委員會隨 CADA 提案一同發布的附屬工作文件（SWD(2026) 502 final），詳細分析了此一境外管轄權問題。

不應將 SEAL 體系與個人資料保護法混淆。歐盟的《一般資料保護規則》（GDPR）是規範應如何收集與處理個人資料的法律，且早已於 2018 年起施行。遵守 GDPR 並不意味著處理該資料之公司的國籍問題也能迎刃而解。無論將資料加密得多麼安全、僅收集所需的最少數量，只要保管該資料的公司是美國法人，在美國政府的法律要求面前，GDPR 的保護就會顯現出局限。GDPR 所規範的是處理資料的方式，而 SEAL 試圖規範的則是處理該資料之公司的國籍與控制權結構。

這兩部法律是從不同的層面看待同一份資料。

歐洲法院過去曾正面遭遇過此一問題。歐盟法院於 2020 年 7 月在所謂的「施雷姆斯二號」（Schrems II）判決中，以美國情報機關可存取通訊資料的美國監控法制為由，裁定歐盟與美國之間的個人資料傳輸協定《隱私盾》（Privacy Shield）無效。該判決的主旨在於：無論在合約中加入多麼嚴密的個人資料保護條款，只要合約相對人受美國法律管轄，就無法透過合約本身來阻止美國情報機關存取資料的可能性。

CADA 決定採用國籍與控制權結構這項遠比合約條款更根本的標準來劃分主權等級，其背景正是累積了這類司法經驗。歐洲獲得的安全教訓，歸根結底在於：實質的防護屏障並非合約條文，而是公司的控制權結構與國籍。

此一教訓亦延伸至市場的反應。亞馬遜、微軟與 Google 近年來紛紛針對歐洲客戶推出各自命名的主權型雲端產品。承諾僅在歐洲內部儲存與處理資料，並限制非歐洲籍員工存取，是這類產品共同的宣傳口號。然而，這類產品極少會將 SEAL 較高層級（即第三階段與第四階段）所要求的控股股權與董事會表決權移交給歐洲。將伺服器位置與營運規範「歐洲化」，與將公司所有權本身「歐洲化」，完全是不同層面的承諾。

SEAL 體系所要做的，正是區分這兩個層面並將其明確列入採購標準之中。

具體案例方面，亞馬遜網路服務（AWS）於 2023 年宣布了一項歐洲主權雲端計畫，另外成立歐洲專用法人，並設立由歐盟公民組成的董事會與高階管理層。這是一項將資料儲存與營運人員保留在歐洲內部的承諾。然而，該歐洲法人的最終股權仍由美國母公司 Amazon.com 掌控。由於 SEAL 第三階段與第四階段所要求的是將此一最終股權結構也轉變為歐盟所有，因此這種型態的主權型雲端產品即使能取得較低層級的資格，也難以跨越較高層級的門檻。

SEAL 的第一階段要求最基本的條件。即資料的儲存與處理必須在歐盟領土內部的設施中進行。此階段適用於國家機密性較低的日常行政業務，包括美資在內的境外企業歐盟分公司，只要在歐洲內部設有資料中心，即可滿足此標準並參與投標。核可方式為供應商自行宣告符合條件的自主證明方式，並不要求額外的第三方審計。

第二階段則超越資料實體存放位置的層面，進一步檢視處理該資料的軟體供應鏈。供應商必須提交詳細記錄軟體組成元件的軟體物料清單（SBOM），並接受原始碼安全性漏洞的驗證。所謂軟體物料清單，是指將一個程式由哪些零件（即哪些外部函式庫與開源元件）所構成詳盡列出的清單。將其理解為類似食品原料標示的概念會更容易明白。

其宗旨在於當某個元件發現資安缺陷時，僅需查看清單即可快速確認該缺陷是否存在於自己所使用的系統中。根據 BISI 的報告，此階段的設計旨在適用於醫療資訊或金融基礎設施等敏感度屬於中等水平的公共服務。即使是境外企業，若與歐洲企業合資以分享控制權結構並證明具備技術隔離機制，亦留有取得此階段資格的管道。

從第三階段開始，條件顯著變得極為嚴格。處理資料的供應企業及其外包企業的總部必須實質設於歐盟領土內，且控股股權與董事會表決權必須掌握在歐盟國籍者手中。維護系統的核心人員亦必須是擁有歐盟國籍的居民，且須通過身分背景調查。據 BISI 報告指出，歐盟委員會在提案中留下了一條例外管道，對於與歐盟簽有情報共享條約且無司法摩擦的盟國，可適度放寬此一要求。此階段適用於國家治安調查網或恐攻威脅分析等與安全直接相關的業務。

盟國例外條款實際上將適用於哪些國家，目前尚未確定。雖然與歐盟已建立情報共享條約及司法合作體系的國家被列為候選國，但具體國家名單並未在提案階段公開。這項模糊之處被視為 CADA 在進行審議期間競爭最激烈的談判焦點之一。若將例外的範圍定得過寬，第三階段的實效性便會削弱；若定得過窄，則必須承受與盟國之間的外交摩擦。

若難以一次想像這四個階段，不妨想想建築物的門禁管制。大廳只要有訪客證，任何人都能進入；辦公室樓層 need 員工證才能進入；伺服器機房僅限獲得額外核准的少數人進入；最深處的金庫室則僅限完成身分調查的極少數人進入。SEAL 的四個階段也與此類似，處理資訊的份量越重，獲准存取的主體範圍就越發收窄。

第四階段是不存在例外狀況的階段。該階段適用於國防、軍事機密、最高層級治安分析等與國家存亡 directly 相關的領域，在完全遵循第三階段之董事會國籍要求與人員條件的同時，對盟國亦不允許任何例外。從系統的設計階段到原始碼的維護，徹底從源頭杜絕外國商業資本干預的空間。供應商必須取得由歐盟網路安全局（ENISA）發行的歐盟網路安全認證體系（EUCS）中最高等級的「高（High）」等級，方能參與投標。這項 EUCS 認證體系並非由 CADA 首創。

據悉，ENISA 多年來一直在籌備這項認證體系，但在最高等級中是否納入限制非歐洲企業持股比例的條款一事上，成員國之間長期存在分歧。以法國為首的部分成員國強烈要求實施持股限制，但其他成員國則持反對意見，認為此類限制會損害市場競爭。CADA 在第四階段要件中明確導入 EUCS High 等級，被視為意圖為先前在認證體系內未能得出結論的所有權爭議增添法律份量。

BISI 報告亦針對這四個階段在實際公共採購中將以何種比例適用提出了推估。在整體公共技術引進專案中，敏感度較低、佔比約達 70% 的一般行政業務被歸類為第一階段。佔比達 20% 的中等敏感度業務則歸類為第二階段。其餘 10% 則劃分為第三階段與第四階段，該報告預測其中 9% 將分配給第三階段，1% 分配給第四階段。有必要說明的是，此推估並非定案統計，而是依據該報告分析所得出的展望。不過，這項比例所傳達的訊息十分明確。

亦即公共採購的絕大多數仍停留在第一階段與第二階段，而要求完全由歐洲持有的第三階段與第四階段，僅適用於整體專案極少數的一部分。

這種分階段設計並非全新的發明。法國早已營運自身的認證體系 SecNumCloud，並對國家最高等級的安全使用案例要求頂級認證，以徹底杜絕美國《雲端法案》（CLOUD Act）的影響力。該認證由法國國家資訊系統安全局（ANSSI）管理，欲取得最高等級的雲端業者被要求須由法國或歐盟資本持有控股股權。BISI 報告評估指出，CADA 的四階段架構是將這種法式認證體系的邏輯擴展至歐盟整體層級的設計。

由於法國已有先前實施的制度，因此 CADA 並非全新的實驗，而是擴展經驗證模型的提案，此一說法因而成立。

除了法國的 SecNumCloud 之外，若干成員國亦各自發展出獨自的認證體系。若各國標準不一，在一國獲得認證的供應商在另一國的採購中就必須從頭接受審查，從而產生效率低落的問題。這正是 CADA 試圖以單一的 SEAL 體系統一這些標準的原因。若二十七個成員國各自堅持不同的認證標準，涵蓋全歐洲的主權雲端市場根本難以成立。

在核准程序中，各階段的比重也不盡相同。第一階段僅憑供應商的自我證明即可通過，並針對中小企業設有免除雙重文件審查的簡易通道。相比之下，從第二階段到第四階段，必須由歐盟指定的獨立第三方稽核機構對系統的原始設計圖進行精密驗證後，再由成員國的專業調查機構給予最終核准。單一成員國作出的核准決定將登錄至歐盟共同登記冊，並經歷為期 60 天、供其他成員國提出異議的相互驗證期。若在此期間異議未能化解，則由歐盟執委會出具最終調解方案以平息爭議，相關程序已在提案之中。

讓單一國家做出的判斷能由全體二十七個成員國重新審視，此一設計旨在防止任何單一國家的鬆散審查成為降低全歐盟安全標準的漏洞。

認證並非取得一次即告結束。若供應商的股權結構或董事會組成發生變化，當初通過 SEAL 等級的前提本身便可能瓦解。若曾獲認證為歐洲企業的公司日後被非歐洲資本收購，該公司所執行的公共合約地位將如何變化，此一問題依然存在。BISI 報告指出 CADA 包含了監控並重新審查此類事後變更的程序，但該重新審查將多久舉行一次、多快執行，目前尚未具體化。

這項等級由誰決定？此一問題亦隨之浮現。公共機構在將新專案交付採購之前，必須先自行診斷該專案所處理資料的敏感度，並判定屬於哪一個 SEAL 階段。若為處理一般行政文書的專案，會被歸類為第一階段；但即便是同一機構，若為處理治安或國防資訊的專案，則可能被歸類為第三階段或第四階段。若此一判定出錯，問題便會事後顯露。若先歸類為較低階段並簽訂合約，事後才確認該資料與國家安全直接相關，便會陷入不得不將已簽訂合約重新大幅修改的困境。

CADA 提案之所以試圖同時規範判定程序與稽核體系，亦可理解為旨在降低此類錯誤歸類的風險。

認證負擔未必僅對大企業而言才較為輕鬆。自第二階段起所要求的軟體物料清單（SBOM）編製與原始碼驗證，都需要投入專責人員與費用。對於資本額不大的歐盟新興雲端企業而言，這項負擔可能會成為阻礙其進入市場本身的障礙。撇開 CADA 為中小企業開放第一階段簡易管道不談，若未能一併制定協助處於成長階段的歐洲企業邁向更高階段的配套支援措施，恐將引發最高階段的市場最終僅對少數已具備資本的大企業開放的悖論。

這套四階段架構若要真正運作，仍有重重障礙需要跨越。歐洲市場目前尚缺乏足以滿足第三階段與第四階段要件的本土企業供應能力，這是多家業界報告共同指出的問題。歐洲企業要滿足這些高階要件之所以需要時間，並非單純是政治意志的問題。要營運大型雲端服務，伺服器硬體、網路及冷卻設備均需要龐大的初期投資，而欲回收該投資，則必須歷經長時間確保穩定的客戶群。

美國的大型雲端公司數十年來早已打造出這種投資與回收的循環鏈。有觀點指出，歐洲企業若想在短時間內追上這條循環鏈，僅靠 CADA 所設定的等級標準並不足夠，還必須同時針對能滿足該等級的企業提供額外的資本支持。無論條件設計得多麼精細，若能通過這些條件的企業不

足，公共機構最終只能退回較低層級的採購，或是依賴例外條款。比起 CADA 所設定的等級本身，能夠達到該等級的歐洲企業能力成長有多快，才是決定這項制度實質成敗的關鍵變數。

根據與參考文獻

1. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), 2026年7月7日.

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, 歐洲聯盟官報, 2026年6月3日, 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, 歐洲聯盟官報, 2026年6月3日.

5. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, 2026年6月23日.

6. Court of Justice of the European Union, Judgment in Case C-311/18 (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems), 2020年7月16日.

4.3 「主權事由解約權」（Sovereignty Termination Clause）與可攜性義務的制度化

無論 CADA 設計出多麼精密的分級制度，若無法回答「如何終止既有合約」這一問題，該分級就只會成為僅適用於新計畫的半套制度。英國的案例最為鮮明地展現了這個問題。

英國國家醫療服務體系（NHS）於 2023 年與帕蘭提爾（Palantir）簽署金額達 3 億 3,000 萬英鎊規模的合約，建置了聯邦資料平台（Federated Data Platform）。該平台是將英國全境醫院的病患資訊、床位現況及輪候名單整合至單一體系進行分析的系統。英國下議院科技委員會發布報告警告指出，這份合約構成國家安全上難以接受的漏洞。左翼媒體 Novara Media 報導稱，多名下議院議員要求政府終止這份合約。問題在於，即使想終止合約，也無法輕易終止。

根據下議院科技委員會的報告，NHS 雖然在整個合約期間持續支付使用費，卻未能取得該系統的核心資產——標準資料模型（Canonical Data Model）與本體論（Ontology）的智慧財產權。合約終止的那一刻，留在 NHS 手中的並非資料，而是只能在帕蘭提爾軟體上運作的資料殘骸。下議院報告亦證實，該合約中所包含的事由解約權條款要到 2027 年 2 月才會生效。這意味著在真正想終止合約的時刻，與實際上能在法律上終止的時刻之間，存在著數年的時間落差。

公共採購合約原本就設有解約條款。常見的有發生違約情況時的解約條款，或是無須特殊理由、僅需支付違約金即可解約的任意解約條款。CADA 打算引進的是有別於這兩者的第三種範疇。亦即即使供應商忠實履行合約，只要判定該供應商的國籍與控制結構對國家安全構成脅威，便能另行建立無須支付違約金即可終止合約的依據。若此類事由未在法律上明確定義，反過來也會給予供應商主張「恣意解約」並提起訴訟的空間。

這個案例所揭露的問題並不局限於帕蘭提爾這家特定公司。一旦公共機構開始將資料託付給特定軟體，該資料就會逐漸被馴化為僅在該軟體的固有結構內才具備意義。將資料遷移至其他系統，絕非僅靠複製檔案就能解決。很多時候必須重新設計承載資料的分類體系與關係結構，亦即本體論本身。所謂本體論，可說是定義各項資訊之間相互建立何種關係的藍圖。例如規定病患、床位與診療紀錄如何相互連結的規則體系即屬於此。

將這套規則體系重新調整以適應其他公司的系統，需要新的合約、開發人力以及相當龐大的預算。合約初期看似低廉的採購，到了轉換的時間點卻要求比初始合約更大成本的悖論便由此產生。業界通常將這種結構性的鎖定效應稱為廠商鎖定（vendor lock-in）。

NHS 案例所展現的鎖定效應並不局限於傳統資料庫。在人工智慧時代的採購中，不僅是資料本身，利用該資料訓練出的模型、調整模型的設定值，乃至用於檢索的嵌入（embedding）都包含在遷移對象中。若供應商將這些要素以專有格式儲存，合約結束後公共機構留下的將只有空

殼基礎設施，而建立於其上的智慧則完封不動地留在供應商手中。有意見指出，CADA 的可攜性義務若要發揮實質效果，就必須制定將這類人工智慧特有資產亦納入遷移對象的細部規定。

在技術上保障可攜性最常見的方法，是強制採用開放標準。若在合約中明確規定資料不得以僅特定公司能讀取的專有格式儲存，而是必須以多種系統皆能共同讀寫的開放格式儲存，那麼即使合約結束，將資料遷移至其他系統的工作也會相對輕鬆。然而，使用開放標準並不意味著像本體論這樣專屬於該系統的設計也會自動轉移。將資料的容器改為開放格式，與轉移該容器內所裝載的知識結構，依然是兩項不同的課題。

「可攜性」這一概念並非完全不存在於歐盟法律中。2023 年通過的歐盟《資料法案》（Data Act, Regulation (EU) 2023/2854）已設有規範雲端與邊緣運算服務之間轉換的條款。該法規定，當雲端使用者從一家服務供應商轉移至另一家供應商時，所被課取的轉換費用將逐步降低，並在指定期限過後完全廢除該費用本身。與 CADA 不同之處在於，《資料法案》是一部已經生效的法規。

若將 CADA 理解為試圖將《資料法案》的可攜性原則擴展至公共採購這一更為敏感的領域，以及主權這一更為沉重的基準，兩部法律之間的關係便清晰可見。如果說《資料法案》旨在保護一般商業雲端使用者免於廠商鎖定，那麼 CADA 則是試圖將這層防護傘擴大至國家機關與公共服務。

CADA 提案所要處理的正是在於此處。歐盟委員會闡明的政策目標之一，即公共機構擁有基於主權理由終止合約的權利，而供應商則承擔在合約終止時，將資料與設定值以開放且具互操作性的格式進行轉移的義務。BISI 報告總結指出，CADA 的三大支柱之一即為此可攜性義務的制度化，其宗旨在於防止公共機構因被特定供應商綁定而喪失議價能力。該條款最終會以何種名稱與條文編號納入最終規章，仍須經歐盟議會與理事會審議後方能確定。

目前所能確認的，僅是歐盟委員會已將此一方向的條款納入提案中，而非已經存在正在執行的規範。

雖然提案中所提及的轉換支援期間具體會是什麼形式尚未定案，但可從已經施行類似制度的其他產業案例中推知一二。電信服務使用者保留原號碼更換電信業者的門號可攜制度，或是轉移銀行帳戶時連同自動轉帳明細一併轉移的帳戶可攜制度，皆屬於此類範例。若將這種構想應用於公共機構的資料可攜，預期將需要舊供應商與新供應商在一段時期內並行運轉系統，並分階段交接資料與業務的程序。

要使這項制度成立，必須同時具備兩個條件。一是從法律上明定解約權，二是確保技術上的可攜性，以便能夠實際行使該解約權。如果 boot 只有法律條文而資料格式依然封閉，公共機構即便擁有終止合約的權利，也沒有運用該權利的方法。反之，即使技術上能夠遷移資料，但合約中設有違約金條款，公共機構也會因為眼前的費用而繼續留在舊系統中。NHS 的案例，正是展現這兩個條件皆未滿足時會發生什麼情況的失敗紀錄。

即使 CADA 實際施行，是否能溯及既往套用於既有合約，仍是另一個問題。一般而言，歐盟的新規多半優先適用於生效日後新簽訂的合約，對既有合約則往往附帶寬限期或單獨的過渡條款。在 CADA 提案最終確定的過程中，如何針對既有合約設定過渡規定，極可能成為成員國之間的談判焦點。對於已多年將資料委託給特定供應商的公共機構而言，若新規無法溯及既往，可能需要很長時間才能切身感受到可攜性義務的效果。

在最初簽訂合約的時間點，這類成本並不顯眼。採購人員通常根據初期引進成本與每年使用費來比較供應商，很少會事先將合約結束後提取資料所需的成本計算在內。這種不對稱性也為供應商創造了相應的誘因。多項市場分析皆指出，在雲端產業中不難觀察到一種策略：先開出低廉的初始價格拿下合約，隨後再拉高轉換成本以留住客戶。CADA 的可攜性義務，可視為試圖從簽約前階段就改變這種誘因結構本身的一項嘗試。

這個問題在小國比在大國表現得更為沉重。人口眾多且財政充裕的成員國，有餘力另行組建專責法律團隊與技術團隊來審查合約。相反地，小成員國的地方政府或小規模公共機構，往往連審查合約的專業人力都顯不足。比起執著於談判，直接接受供應商提供的標準合約對眼前來說更為便利。這種不對稱性一旦累積，即使事由解約權存在於法典中，在有能力實際行使該權利的機構與缺乏能力的機構之間，依然會產生差距。

有觀點指出，基於與 CADA 提案為中小企業供應商開闢簡易核准通道類似的邏輯，預先為簽約的公共機構準備好標準化的可攜性要求與合約範本，才是縮小談判力差距的解決之道。

轉換成本的問題在合約結束後依然持續。撇開遷移資料的工作不談，處理該資料的人員熟悉新系統同樣需要時間與預算。由於公共機構的預算週期通常以單一年度為單位編列，往往難以一次性籌措需跨多年分攤的轉換成本。因此，即使法律上存在事由解約權，但因預算部門無法負擔轉換成本而被迫實質延長合約的案例，已在多個國家被報導。CADA 提案在規定可攜性義務的同時亦擬定轉換支援期間，顯然也是考量到這類現實障礙的制度設計。

在法律中明定事由解約權與可攜性義務，還會引發另一層法律緊張關係。歐盟公共採購指令（Directive 2014/24/EU）以及歐盟簽署的世界貿易組織《政府採購協定》，原則上規定在採購過程中不得不當歧視具備資格的外國供應商。雖然以國家安全與國防為由的例外條款是以《歐盟運作條約》第346條為依據，但該例外本質上是被設計為例外，而非原則。

若 CADA 在 SEAL 的高級階段產生實質上將非歐洲企業排除於採購之外的效果，則該項排除是否屬於安全例外的正當範圍之內，恐將引發後續的法律爭端。這股緊張關係，在 CADA 經由歐洲議會與歐盟理事會審議期間，勢必成為針對每一字條文用語持續論辯的議題。

還有另一個數字能讓人衡量這個問題的份量。帕蘭提爾（Palantir）在 2026 年第二季的財報中宣布，其營收成長率較去年同期高達 93%。據德國媒體 Netzpolitik 報導，當歐洲各國宣示要在本國治安與國防領域與帕蘭提爾保持距離之際，歐洲的投資銀行與資產管理公司卻已投入數

十億歐元購買帕蘭提爾的股票。從公共採購的大門將其推開，卻又從金融市場的視窗注入資本，這種矛盾絕非僅憑單一法律條文就能解決。

我們亦不能忽視，可攜性義務是一項不具特定方向性的工具。讓資料能夠輕易遷移的規定，不僅開闢了轉向歐洲企業的路徑，也同時打開了轉向其他美國企業的大門。事由解約權與可攜性義務本身，比起偏袒特定國籍企業的機制，更接近於整體提升公共機構談判力的裝置。要讓該談判力最終轉化為選擇歐洲企業的實際結果，歸根究底仍須仰賴 SEAL 體系所規定的國籍與治理結構要件共同發揮作用。

在捍衛主權的宣示與支撐該宣示的歐洲本土替代軟體實際供應能力之間，依然存在著鴻溝。CADA 的解約權與可攜性義務，正是為了填補這道鴻溝所邁出的制度第一步。這第一步能否在實際採購現場發揮作用，將取決於歐洲議會的審議結果及其後的施行過程。

依據及參考文獻

1. 英國下議院科學技術委員會, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', House of Commons, 2026年.

2. Novara Media, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026年.

3. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), 2026年7月7日.

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, 2026年.

5. Jan Ebert(揚·埃貝爾), 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026年.

6. European Union, Regulation (EU) 2023/2854 (Data Act), Official Journal of the European Union, 2023年.

5.1 弗朗切斯卡·布里亞的「歐洲堆棧（EuroStack）」構想與 3,000 億歐元的投資障壁

弗朗切斯卡·布里亞是一位義大利裔經濟學家，曾擔任歐盟委員會顧問。她曾任巴塞隆納市政府數位創新委員，推動由城市本身而非私營企業來管理市民所產生數據的政策。這段經歷成為她日後在規劃歐洲層面的數位政策時，屢次引用的基準點。布里亞在多次發言與文章中表達了擔憂，認為將公共基礎設施轉交給美國私營科技企業的趨勢，可能會動搖民主的根基。

本書前幾章所探討的事件——即法國國內安全總局（DGSI）擺脫 Palantir，或是 Anthropic 遭到封鎖存取的事件——皆可視為證明此一擔憂並非空泛抽象的具體實例。布里亞在構想歐洲堆棧時反覆強調的核心，亦非合約中的條款，而是「究竟由誰擁有並控制基礎設施本身」這一問題。

據調查報導媒體 Follow the Money 報導，布里亞透過名為「威權堆棧（The Authoritarian Stack）」的獨立研究，剖析了歐洲投資銀行與資產管理公司向 Palantir 等美國企業注入巨額資本的趨勢。她指出了其中的矛盾之處：歐洲的退休基金與銀行，反而向侵蝕本國公共基礎設施的企業提供資金。這項指責與本節後文將討論的歐洲內部投資資本流向問題相呼應。

將此一擔憂轉化為具體藍圖的產物，便是《歐洲堆棧報告》。其正式名稱為《EuroStack – A European Alternative for Digital Sovereignty》，由布里亞、保羅·蒂默斯與法烏斯托·格爾諾內共同撰寫。德國私營基金會貝塔斯曼基金會於 2025 年 2 月 13 日發布了該報告。貝塔斯曼基金會是由德國大型媒體集團貝塔斯曼成立的非營利基金會，長期資助歐洲社會與經濟政策的研究。

該基金會發布《歐洲堆棧報告》這件事意味著，此報告並非歐盟的官方文件，而是由政策研究基金會資助的獨立倡議書。首先必須釐清這一事實。「歐洲堆棧」並非歐盟採納的法律或政策。它是民間基金會發表的政策建議書，係作者群促請歐盟與各成員國政府朝此方向採取行動的文件。本章所提及的數據與設計，均為該建議書中所包含的內容，閱讀時應與實際執行中的預算或已頒布的規範加以區隔。

第四章討論的《雲端與 AI 開發法》（CADA）與這份報告處於不同的層次。CADA 是歐盟委員會向歐洲議會與歐盟理事會提交的規章草案，目前正處於正式立法程序中。而「歐洲堆棧」則是位於該程序之外的民間基金會政策報告。若說 CADA 旨在處理在歐洲境內興建資料中心以及審查營運企業國籍的問題，那麼「歐洲堆棧」則是範圍廣泛許多的構想，主張從半導體到人工智慧的整個七層結構全面實現自立。

兩份文件雖然共享實現歐洲技術自立的共同目標，但一份是正在進行立法程序的規章草案，另一份則是在該程序之外指引方向的政策建議書，因此兩者的法律份量截然不同。

布里亞在解釋「歐洲堆棧」構想時，經常將其比作歐盟單一貨幣「歐元」的引進。這項比喻旨在說明：正如過去各成員國使用不同貨幣時，歐洲打破了貨幣壁壘並建立共同金融秩序一樣，在數位基礎設施領域，也必須將分散於各成員國的能力凝聚在一起。考量到歐元的引進經歷了長達數年的談判與條約修改，這項比喻亦可解讀為強調「歐洲堆棧」所追求的整合規模十分龐大。

報告將歐洲的數位基礎劃分為七個層級。最底層是用於製造半導體與電池所需的原材料，以及運作資料中心所需的能源與水資源。在其之上，依序堆疊著半導體晶片製造層、寬頻通訊網絡鋪設層、感測器與物聯網裝置製造層，以及雲端基礎設施營運層。最頂層則是軟體層與數據暨人工智慧層。報告主張，在這七個層級中，只要有任何一個層級由歐洲以外的企業所掌握，建造於其上的其餘層級便無法達成真正的完全自立。

其邏輯在於，即使在國內生產半導體，若搭載該半導體的伺服器只能在美國公司擁有的資料中心內運作，那麼自立便僅算完成了一半。

若將這七層結構比喻為蓋房子的順序便容易理解。無論用多麼堅固的材料砌牆，若屋頂必須按照別人的設計圖購買，整棟房屋的安全便取決於賣屋頂的人手中。《歐洲堆棧報告》所指的自立亦是同理。報告的核心論點在於，即使半導體、通訊網路乃至雲端皆由歐洲企業打造，但若在其上運行的 AI 模型與數據管理軟體仍依賴美國企業的產品，那麼下層六個層級所取得的成果，便可能僅因最頂端的一個層級而產生動搖。

報告同時提議將這七個層級結合，直接向市民提供五項共同服務。分別為：在歐洲境內處理運算的主權雲端服務、確認市民身分的數位身分證皮包、無須銀行手續費即可支付的數位歐元支付體系、在各成員國之間安全傳輸數據的聯邦數據空間，以及由歐洲親自設計與營運的人工智慧引擎。這五個領域目前均依賴美國或其他境外企業的服務，報告指出，擺脫此種依賴正是「歐洲堆棧」構想的實質目標。

在這五項服務中，與市民日常生活最為貼近的是數位歐元支付體系。目前在歐洲使用刷卡支付時，交易資訊大多會經過美資信用卡公司的支付網路。商家每次接受刷卡支付時所繳納的手續費中，有相當大的一部分流向了擁有該支付網路的公司。報告所提議的數位歐元體系，旨在將此支付網路本身置於歐洲中央銀行體系之內，從而防止交易資訊流向境外，並改變手續費結構。數位身分證皮包亦是出於類似的問題意識。

其核心在於，取代現今市民在線上驗證身分時必須透過特定大型科技企業登入系統的慣例，改由國家直接建立並管理身分驗證機制。值得一提的是，在這五項服務中，唯獨「數位身分證皮包」並非由《歐洲堆棧報告》首次提出的概念。歐盟早已於 2024 年採納了歐洲數位身分規章，即所謂的 eIDAS 2.0，強制要求各成員國向市民提供歐盟數位身分皮包。該規章是獨立於《歐洲堆棧報告》之外、業已制定並實施的法律。

《歐洲堆棧》報告並非主張廢除此一現行制度並重新建立，而是更傾向於建議將這股已在進行中的趨勢納入七層結構之中，使其與其他層級有機連結。其餘三項服務則較接近政府與企業所面臨的層位。主權雲端服務與第四章討論的 CADA 主權保證等級體系在目標方向上有所重疊。

與亞馬遜網路服務或微軟針對歐洲客戶推出的所謂主權型雲端產品不同——正如第四章所述，這些產品存在著未能將控股權移交給歐洲的局限——《歐洲堆棧》所指的主權雲端服務，則是指所有權本身即屬於歐洲的雲端。聯合資料空間是讓成員國政府與企業在傳輸資料時無需經過美國雲端的管道。這一構想與第四章討論的 CADA 相比出現得更早，且與 2019 年由法國與德國啟動的 Gaia-X 計畫一脈相承。

不同於 Gaia-X 被評為僅止於缺乏法律約束力的自願性標準化嘗試，《歐洲堆棧》報告建議將此資料共享體系提升為由國家預算支持的共同基礎設施。主權人工智慧引擎則旨在改變目前歐洲公共機構與企業依賴美國或其他境外企業所開發的大型語言模型的現狀。

報告提出的投資規模不可謂不大。作者群估算建立這七層基礎設施大約需要 10 年時間，並指出到 2035 年為止需要總計高達 3,000 億歐元的資金。此外，報告還包含了設立一項規模為 100 億歐元的獨立技術基金作為早期引導資金的建議。將 3,000 億歐元均攤至 10 年，意味著每年平均需要持續進行 300 億歐元規模的投資。該數據為報告作者的估算結果，並非歐盟官方正式採納或編列的預算。

將這一金額與歐盟目前實際運作的預算並列比較，其中的差距便顯露無遺。政策研究機構 CERRE 於 2025 年 9 月發布的報告指出，在歐盟推動的競爭力基金中，分配給數位主權相關項目的預算約為 550 億歐元。與《歐洲堆棧》報告要求的 3,000 億歐元相比，還不到其五分之一。競爭力基金是歐盟擬在 2028 年起實施的下一階段多年期財務架構中，為強化數位與產業競爭力而擬編列的預算項目，目前仍等待成員國與歐洲議會的最終批准。

這意味著該預算本身亦非確定金額，且其中配給數位主權的份額遠低於《歐洲堆棧》所要求的數額。這項比較所傳達的訊息非常明確：《歐洲堆棧》是一份指引方向的藍圖，並不代表完成該藍圖所需的預算已經到位。

以布里亞為首的歐洲政策討論參與者指出，填補這一資金缺口的來源並非政府預算，而是民間儲蓄。據媒體《EU Perspectives》2026 年 1 月的報導，截至 2026 年，歐盟家庭存於銀行帳戶的存款總額已超過 30 兆歐元。世界經濟論壇於 2026 年 1 月年會討論中提及的數據顯示，該金額已超過歐盟整體國內生產毛額的兩倍。問題在於這筆資金處於停滯狀態。

據《Politico》歐洲版於 2026 年 6 月 4 日報導的討論內容，雖然像瑞典這樣有超過半數公民投入資金於股票或基金的國家存在，但在歐洲許多大型成員國中，該比例僅停留在 2% 左右。該討論指出，鎖在銀行的資金無法流向新創企業，而真正用於投資的資金大部分反而流向了美國的大型科技股。

退休基金也面臨著類似的問題。據《法國 24》於 2026 年 6 月播出的討論節目所指出，歐洲的退休基金受限於以穩定性為優先的監管規定，難以向處於早期成長階段的科技企業提供資金。像歐盟的保險與退休金監管體系《償付能力二號》（Solvency II）這類規定，要求退休基金必須保持一定比例以上的安全資產，以防遭受突發性損失。

這項規定的宗旨雖在於保護退休人員的養老資金，但結果卻同時造成了限制退休金流入高風險且收益不確定的早期成長型科技企業。這種資金緊縮進一步導致了人才流失。同場討論中亦提到，無法獲得資金支援的歐洲科技人才紛紛流向美國矽谷。歐盟委員會隨 CADA 提案一同發布的工作文件 SWD(2026) 502 final，亦透過數據揭示了這一資金差距。

在全球創投投資總額中，歐洲所佔比例僅為 5%，而美國則高達 52%。布里亞在 2024 年 CEPS 演講中指出，歐洲孕育出的成功新創企業中，有相當一部分在擴大業務規模的階段被外資收購，從而流失至歐洲境外。

基於此診斷，布里亞一直要求進行稅制改革，引導銀行存款與退休金資產流向歐洲科技企業。被提及的方案包括：對將資金投入國內科技企業而非長期定存的公民給予減稅優惠，或者放寬退休基金投資於風險資產的上限。此類建議是否已促成實際立法，在本書所查核的資料範圍內尚未確定。該報告的邏輯在於，若欲將《歐洲堆棧》報告所要求的 3,000 億歐元中的相當一部分由民間資本而非政府預算填補，則此類稅制改革必須先行。

資金也並非完全沒有流動。據法語經濟媒體《ÉcoQuick》2026 年 6 月 4 日報導，歐盟已確定撥款 200 億歐元公共資金用於興建人工智慧超巨工廠。西班牙首相府於 2026 年 7 月 1 日發布聲明稱，已批准一項投入 7 億 2,000 萬歐元公共預算興建該國人工智慧超巨工廠的協議。據媒體《Startup Online》2026 年 5 月 21 日報導，由瑞典資產管理公司 EQT 負責營運、規模達 50 億歐元的 Scale-Up Europe 基金亦預計於 2026 年秋季開始撥付資金。

該基金將與由德國復興信貸銀行（KfW）籌集、規模達 10 億歐元的深科技基金協同運作。

即便將這些實際執行的金額全部相加——200 億加上 7 億 2,000 萬與 50 億——總額仍未達 300 億歐元。這僅為《歐洲堆棧》報告要求的 3,000 億歐元的十分之一。歐盟與部分成員國確實付諸了實際行動，但其規模距離填滿布里亞所提出的藍圖仍相去甚遠。

將these數字並列來看，問題 glance 的性質變得更加明確。歐盟家庭存於銀行的存款超過 30 兆歐元，而 EuroStack 報告要求的投資額則為 3,000 億歐元。純粹從算術角度來看，這意味著只要將這些存款 glance 的 1% 轉向科技投資，就足以補齊報告要求的全部金額。問題在於，目前尚未具備能引導這 1% 資金移動 glance 的誘因與制度。這項差距 glance 的本質更接近於：並非缺乏資金，而是缺乏能將資金從儲蓄轉移至投資 glance 的稅制、金融產品以及信任。

若這項差距無法縮小，EuroStack 所描繪 glance 的七個層級中，相當一部分將不可避免地停留在設計圖階段。越是像半導體或資料中心這樣需要龐大初期投資 glance 的層級，就越先受到資金短缺 glance 的影響。這正是為何有人指出，僅憑目前按成員國劃分編列預算 glance 的方

式，難以承擔規模達 3,000 億歐元 glance 的計畫；也是布里亞試圖引進民間儲蓄乃至退休金資產 glance 的原因。

歐盟在 2028 年展開 glance 的下一輪預算談判中，能將數位主權預算增加多少，預計將成為評估 EuroStack 構想能否從設計圖邁向實際計畫 glance 的下一個試金石。在該談判結果出爐之前，EuroStack 仍是一幅指引歐盟前進方向 glance 的地圖，而非一座已經竣工 glance 的建築。

根據與參考文獻

1. Francesca Bria, Paul Timmers, Fausto Gernone, 'EuroStack – A European Alternative for Digital Sovereignty', Bertelsmann Stiftung, 2025年2月13日, https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty

2. Johanna Bröer 等, 'Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?', CERRE Issue Paper, 2025年9月, 17頁.

3. Joana Soares, 'Your cloud data lives on American servers. Brussels is moving to act', EU Perspectives, 2026年1月.

4. World Economic Forum, 'Is Europe's Tech Sovereignty Feasible?', WEF Annual Meeting 2026, 2026年1月.

5. POLITICO Europe, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, 2026年6月4日, 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, 2026年6月.

7. European Commission, SWD(2026) 502 final, 歐盟公報, 2026年6月3日, 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, 2024年.

9. 羅伊克·克拉夫特 (Loïc Kraft), 'Souveraineté numérique : Bruxelles renâcle à imposer des contraintes trop fortes', 艾科快報 (Écho Quick), 2026年6月4日.

10. 西班牙首相府, 'The President calls for public-private partnership to drive forward Spain's artificial intelligence gigafactory', La Moncloa, 2026年7月1日.

11. Startup Online 編輯部, '歐盟數位主權之算力·雲端·開源·資本研究報導', Startup Online, 2026年5月21日.

5.2 替代軟體聯盟：阿卡迪亞（Arcadia）與開源數位公共財

指揮管制系統（通常簡稱為 C2）這類軟體，是將戰場上發生的事集中顯示於螢幕，並將指揮官的命令傳達給部隊的工具。它能即時整理並顯示哪支部隊在何處、發現了什麼目標，以及向哪支部隊下達了何種命令。若第三章探討的 Maven 智慧系統在北約盟國層面上承擔了這一角色，阿卡迪亞則是法國嘗試以自研軟體取代相同角色的努力。

法國正在開發一套由本國主導的軍用人工智慧指揮管制系統，以取代 Palantir 的 Maven 智慧系統。其名稱為阿卡迪亞。根據國防媒體 Armees.com 與 Économie Matin 於 2026 年 7 月 9 日的聯合報導，阿卡迪亞是由泰雷茲、空中巴士、賽峰以及法國大型語言模型開發商 Mistral AI 組成聯盟共同研發的戰場指揮軟體。Command AI 與 Impact 等戰術軟體新創公司也加入其中。

Mistral AI 於 2023 年在巴黎成立，是一家大型語言模型開發商，被評為歐洲最領先的人工智慧企業之一。該公司參與軍用企業聯盟的事實表明，歐洲的民間人工智慧產業正在與國防領域走向結合。

阿卡迪亞並非無中生有的專案。根據同一報導，法國先前亦曾多年推動由泰雷茲與 Sopra Steria 共同進行的戰鬥指揮所系統 SIA C2，卻因技術不相容問題而導致計畫取消。阿卡迪亞聯盟汲取了這一失敗的教訓，從一開始就將系統設計為模組化架構。透過採用開放式介面（API），讓多家公司製作的軟體組件得以互相結合，並同時滿足了支援盟軍之間無線通訊的北約聯軍任務網路（FMN）標準。

FMN 是北約成員國不同的指揮管制系統在聯合作戰中交換資訊所設定的共通規格。讓某一國家部隊透過自國系統確認的目標資訊，在遵循 FMN 標準的其他國家系統中也能以相同格式讀取，正是該標準的目的所在。阿卡迪亞符合這一標準，意味著法國在採用獨立軟體的同時，並未放棄與盟軍共享資訊的能力。這是旨在同時滿足國家自主設計權與盟軍間相互操作性的設計。

所謂模組化設計，是指並非整套購買單一大型成品，而是從多家公司採購標準化的組件進行組裝的方式。即使製造某一組件的公司倒閉或終止合約，只要更換為符合相同規格的其他公司組件，整體系統便能持續運作。與先前的 SIA C2 計畫受制於特定供應商的封閉式設計不同，阿卡迪亞憑藉這種模組化結構，旨在降低整體系統被單一企業的狀況所牽制之風險。

CWIX 是代表聯軍相互操作性演習的北約例行活動，每年用於檢驗成員國研發的武器系統與通訊設備是否能在實務上相互連動。在該演習中測試新開發的指揮管制軟體能否與盟軍的其他設備進行實際通訊，已成為慣例。阿卡迪亞於 2026 年 6 月在波蘭比德哥什舉行的這項演習中首次進行試運作。根據國防專業媒體 Defense News 於 2026 年 6 月 5 日的報導，該演習是驗證阿卡迪亞在實戰環境下資料處理能力的場合。

這意味著並非將完成的系統全面部署於實戰，而是在北約標準下對開發中的系統進行測試的階段。根據同一報導，法國陸軍副參謀長派翠克·茹斯特爾將軍在該演習中表示，未經驗證就接受外國軟體的態度無異於自行讓渡國家主權，並說明阿卡迪亞是法國對美國軍事技術優勢的回應。

阿卡迪亞與 Maven 的開發方式存在顯著差異。Palantir 採取了單一供應商模式，將 Maven 智慧系統開發為由其擁有的軟體並供應給北約。相反地，阿卡迪亞則採用了聯盟模式，由泰雷茲、空中巴士、賽峰、Mistral AI 以及多家新創公司將各自的專業領域製作成模組後進行結合。這是為了防止單一公司掌握整個系統的主導權所做的設計。雖然這種模式有著可能放緩開發速度的缺點，但也有著能降低將整體安全基礎設施過度依賴單一企業之風險的優點。

這一趨勢並不局限於法國。根據媒體 The Next Web 於 2026 年 7 月 18 日的報導，法國與德國政府共同承諾，將攜手建立一套能與 Palantir 的軍用人工智慧軟體抗衡的歐洲層級競爭體系。這項承諾是否已轉化為具體的共同開發計畫，抑或各國僅止於各自繼續推進如阿卡迪亞般的獨立專案，根據本書所查證的資料尚不明確。根據顧問公司 Pathfounders Group 於 2026 年 4 月整理的清單，在歐洲內部被視為 Palantir 替代方案的企業，除了參與阿卡迪亞聯盟的公司之外，還有數家企業。

這意味著與其由單一勝者決定一切，不如說正形成一種由多家企業在各自領域相互競爭的格局。

截至目前，阿卡迪亞是由法國主導的專案，參與聯盟的企業也大多是法國公司。CWIX演習雖然是北約成員國共同參與的多國活動，但阿卡迪亞本身並未獲採納為整個北約的官方標準。法國以外的其他成員國是否會實際引進此系統，還是各國會各自使用本國開發的獨立系統，在本書所查證的資料範圍內，目前尚未確定。如果歐洲各國分別開發彼此不同的指揮管制系統，這一次歐洲國家之間的互操作性可能會成為新的課題。

該聯盟中賽峰（Safran）所承擔的角色值得另行探討。根據法國經濟媒體 L'Essentiel de l'Économie 於 2026 年 6 月 8 日的報導，以航空發動機製造起家的賽峰自 2022 年起相繼收購了多家情報分析相關企業。2022 年 7 月，賽峰以 1 億 100 萬美元收購了能在干擾環境下提供精確定位訊號的 Orolia；2024 年則以 2 億 2,000 萬歐元併購衛星影像分析企業 Preligens，並成立全新的 Safran.AI 部門。2026 年 2 月，賽峰進一步收購了掌握地下空間抗干擾技術的 Syntony；2026 年 5 月又收購了雷達影像分析企業 Kayrros 的國防部門。

據同一報導指出，賽峰集團AI部門擁有300名工程師，2025年營收較前一年成長了65%，並預估2026年將實現90%的成長。該媒體報導，該部門開發的目標識別引擎ACE，亦被用於與新加坡、加拿大及印度的合作夥伴簽署共同開發協議。這份合作國名單所代表的意涵相當值得關注。新加坡與印度雖未加入由美國主導的情報共享聯盟「五眼聯盟」，卻是一直與西方保持安全合作的國家。

賽峰與這些國家攜手合作，可解讀為試圖在以美國為中心的情報聯盟之外，拓展獨立的情報合作網絡。這家原本製造航空引擎的公司，在短短幾年內接連收購情報分析企業，轉型為人工智慧企業，這一案例也呈現出歐洲國防巨頭放棄自行開發軟體與數據能力，轉而透過收購快速掌握相關能力的趨勢。

在軍事領域之外，以開源軟體為核心的行動亦在積極推進。歐盟委員會於2026年6月3日發布的官方文件 COM(2026) 503 final 估算，歐盟成員國每年支付給美系軟體訂閱費的金額高達2,640億歐元。為了減少這筆龐大支出，該文件提出了一項開源策略，強調「公共預算、公共程式碼」的原則，主張將以公共預算開發的軟體原始碼免費向公眾開放。

這筆費用之所以年年重複產生，根源在於軟體產業特有的鎖定效應。一旦政府機關開始使用特定公司的辦公軟體建立並儲存文件，即便幾年後想換成其他公司的產品，由於檔案格式與業務流程早已適應了該公司的規格，轉換成本就會如雪球般越滾越大。比起每年支付的訂閱費，這筆轉換成本帶來的負擔更為沉重，使得政府機關只能選擇繼續續約。而開源策略所針對的，正是這種鎖定結構本身。

其邏輯在於，透過公開原始碼讓多家企業在相同的程式碼基礎上展開競爭，就能避免受制於單一供應商。

基於這項原則，法國、德國、義大利與荷蘭政府於2025年10月組成了名為「數位公有地 EDIC」的歐洲數位基礎設施聯盟。EDIC是歐洲數位基礎設施聯盟（European Digital Infrastructure Consortium）的縮寫，是多個成員國推動共同計畫時採取的法定組織形式。各國政府無需各自簽訂合約，而是由該組織統一代表參與國籌措預算並管理計畫。該聯盟的核心，正是德國聯邦內政部批准開發、作為 Microsoft 365 替代方案的辦公協作軟體 openDesk。

openDesk 是將檔案儲存工具 Nextcloud、郵件伺服器 Open-Xchange、內容管理工具 Drupal 與分散式即時通訊軟體 Matrix 整合在一起的軟體套件。各地方政府並非各自修改原始碼，而是透過名為 openCode 的共享儲存庫共同管理原始碼。據德國採購專業媒體 Cosinex 部落格報導，這項開源策略正與被稱為「僅一次原則」（Once-Only）的行政原則一同推進。「僅一次原則」旨在讓民眾或企業提交一次文件或資訊後，各政府機關即共享該資料，無需向多個機關重複遞交。

共享原始碼的 openCode 與共享行政資訊的「僅一次原則」，處理的對象雖異，卻出自減少重複、共享資源的同一概念。據相關報導指出，法國的協作軟體 La Suite、德國的 openDesk 以及荷蘭的 MijnBureau 成功實際演示了這三個不同國家的軟體能在不經由外國雲端服務的情況下互相傳輸文件。這場演示的意義非同小可。在此之前，不同國家的公務員若要互傳文件，最終往往只能匯聚到同一個美系雲端服務帳戶之中。

三國展現出即使各自採用不同的軟體也能彼此連通，意味著歐洲國家不必統一使用單一軟體，同樣有辦法確保系統間的互操作性。

這項開源策略預估也將與第四章所探討的 CADA 主權保證等級體系相互銜接。像 openDesk 或 La Suite 這類一般行政軟體，很可能屬於 SEAL 體系中敏感度相對較低的低階層級；而像 Arcadia 這類與國防直接相關的軟體，則較可能適用高階層級的嚴格要件。然而，開源軟體與 SEAL 等級體系實際上將如何相互銜接，仍需視 CADA 在擬定最終條文時的具體化情況而定。

地方政府層級亦有相關案例。根據歐盟委員會「可互操作歐洲」（Interoperable Europe）入口網站整理的資料，德國北部的什勒斯威格-霍爾斯坦邦自2020年起，展開了將2萬5,000台公務電腦中的 Microsoft 作業系統與 Outlook 移除、全面轉換為 LibreOffice 的工作。根據該邦政府於2025年12月4日發布的新聞稿，這項轉換使邦政府每年節省了1,500萬歐元的軟體授權費用。

瑞士則透過立法走得更遠。根據瑞士媒體 Watson 於2024年12月4日的報導，瑞士於2024年通過了《電子政府電子手段法》（EMBAG），強制規定原則上以公共預算開發的所有軟體原始碼皆須開源公開。根據該法，瑞士聯邦軍參謀部網路司令部將自行開發的安全分析軟體 Loom 免費向民間開放。軍方將自研軟體作為開源釋出的案例極為罕見，從這一點來看，該決定凸顯了瑞士意圖將本國技術自主推進到何種地步。

這股趨勢與第一章所探討的法國對內安全總局（DGSI）轉用 ArgonOS、德國聯邦憲法保衛局脫離 Palantir 屬於同一脈絡。第一章討論的是國內情報機關將原先由 Palantir 承擔的業務移轉至其他供應商產品的決策；相比之下，本節所探討的 Arcadia 與 openDesk 則是歐洲試圖自行研發出替代品的開發計畫。改變採購來源的決定，與創造出可供替換的產品本身，是屬於不同階段的課題。

Arcadia、openDesk 與 EMBAG 是在不同層面運行的項目。Arcadia 處理軍事指揮管制軟體，openDesk 處理公共行政辦公軟體，EMBAG 則處理將原始碼公開義務法制化的工作。這三者共享的交集只有一個：與其租賃外國企業的商業產品，不如在歐洲內部打造能夠擁有並自行修改原始碼的軟體。

這項判斷究竟會普及到何種程度，仍有待觀察。雖然有像什勒斯威格-霍爾斯坦邦或瑞士聯邦軍這樣取得顯著成效的案例，但並非所有歐盟成員國都以相同的速度投入開源轉型。越是早已深深牽連於微軟或 Google 軟體的政府機關，轉型所需的初期成本與員工重新培訓負擔就越大，而承擔此負擔的政治意願在所有成員國中也並未達到相同的程度。阿卡迪亞與 openDesk 所展現的是一種可能性，而非橫跨整個歐洲的完整轉型。

根據與參考文獻

1. Jean-Baptiste Le Roux, 'Cloud de combat : face à Palantir, la France veut faire émerger un champion national des logiciels militaires', Economie Matin, 2026年 7月 9日.

2. Jean-Baptiste Leroux, 'IA de combat : face au Palantir, la France veut son Maven hexagonal', Armees.com, 2026年7月9日.

3. Rudy Ruitenberg, 'France to test its own AI-powered battlefield command in June NATO exercise', Defense News, 2026年6月5日.

4. L'Essentiel de l'Éco 編輯部, 'Comment Safran devient un géant du renseignement par IA', L'Essentiel de l'Éco, 2026年6月8日.

5. European Commission, COM(2026) 503 final, 歐盟公報, 2026年6月3日, https://ec.europa.eu/newsroom/dae/redirection/document/129100

6. Digital Independence Editorial, 'Digital Sovereignty in Europe', Digital Independence, 2026年2月16日.

7. European Commission, 'Open source progress in Schleswig-Holstein', Interoperable Europe Portal, 2026年.

8. 什勒斯維克-霍爾斯坦邦政府, 新聞稿, 2025年12月4日.

9. Watson 編輯部, 'Schweizer Armee setzt auf europäische Software statt Microsoft', Watson, 2024年12月4日.

10. TNW 編輯部, 'France and Germany pledge to build a European rival to Palantir's military AI software', The Next Web, 2026年7月18日.

11. Pathfounders Group, 'Here are the top five companies vying to take on Palantir in Europe', Pathfounders Group, 2026年 4月.

12. Wolf Witte, 'Vergabebeschleunigungsgesetz und digitale Souveränität 2026', cosinex Blog, 2026年5月21日.

5.3 對抗避稅跨國企業的經濟主權：CICTAR 報告與公共財政保護

歐洲各國政府每年都向帕蘭提爾（Palantir）等美國企業支付巨額採購預算。2026年8月5日發表的一份報告，探討了這筆支出究竟有多少能以稅收形式回饋歐洲社會。國際企業租稅責任研究中心（CICTAR）是一個長期追蹤跨國企業避稅結構的研究機構，在帕蘭提爾之前，就曾發表過分析多家跨國企業租稅慣例的報告。這次則將研究對象縮小至帕蘭提爾。

這份在歐洲公共服務工會聯盟（EPSU）資助下完成的報告，透過分析 Palantir 的稅務結構，主張該公司相較於從公共合約中獲得的利潤，所繳納的稅金極少。這項內容由調查報導媒體 Follow the Money 於 2026 年 8 月 5 日撰文報導。EPSU 是代表公共部門勞工的歐洲層級工會聯盟。由於以 Palantir 為首的私營企業擴大公共採購規模的趨勢，會直接影響公共部門的工作機會與預算，因此有必要說明 EPSU 對這項調查提供資助屬於利益相關者的支持。

雖然這一事實並不會自動使報告的分析內容失效，但這是讀者在閱讀該報告時值得參考的背景。

該報告探討德國案例的背景，源於實際的警察採購合約。據德國媒體 LabNet Germany 報導，包括黑森州在內的多個德國州警察，一直使用 Palantir 的軟體來追蹤與分析潛在威脅人物（德語稱為 Gefährder）。報導解釋道，此類合約在多個州累積，成為了 CICTAR 推算德國境內稅源損失規模的背景。

所謂有效稅率，是指企業實際繳納的稅金除以稅前利潤所得出的數值。無論法定稅率有多高，如果透過各種扣除與會計手段使實際繳納的稅金減少，有效稅率就會隨之降低。CICTAR 報告所指責的並非 Palantir 違法，而是其層層動用合法的會計手段來拉低有效稅率。違反稅法的逃漏稅，與在稅法允許的程序內減少稅金的避稅，在法律上屬於不同的範疇。該報告舉發的是後者。這種區分也影響著處理該問題的方式。

逃漏稅是調查與懲罰的對象，但避稅並非透過懲罰個別企業就能遏止的問題。這意味著需要採取制度性的對應措施，例如修改稅法本身、重新構建國家間的稅務協定，或是變更採購合約的條件。本章後文將探討的 BEFIT 提議以及修訂採購規格書的要求，即屬於此類制度性對應措施。

CICTAR 報告主張 Palantir 在 2025 年的全球企業所得稅有效稅率僅為 1.4%。根據報告，Palantir 在 2025 年一整年賺取了約 16 億 6,000 萬美元的稅前利潤，但向全球繳納的企業所得稅僅為 2,270 萬美元。此數據源自 CICTAR 與 Follow the Money 的分析，本書並未另行驗證 Palantir 的原始財務報表。不過，這項主張所指出的問題本身仍有探討的必要。

這項由經濟合作暨發展組織主導、140 多個國家參與的協議被稱為「第二支柱」（Pillar Two），在 2021 年達成整體架構協議後，正由各參與國陸續納入國內法中。無論跨國企業在哪個國家營

運，該協議的目標皆為課徵至少 15% 的企業所得稅。若 CICTAR 報告提出的 1.4% 數據屬實，這無疑是一個嚴重偏離該國際協議宗旨的結果。

美國稅務政策研究機構 ITEP 於 2026 年 3 月 22 日發布的另一份報告分析指出，Palantir 利用川普政府時期制定的稅務優惠法案中的研究開發費即時扣除條款，實際上並未繳納美國境內的聯邦企業所得稅。

CICTAR 報告還介紹了 Palantir 所使用的會計手段。在跨國企業的總公司與海外分公司之間，經常存在著所謂的移轉定價。這是分公司以技術授權費或服務手續費的名義向總公司匯款的交易。該金額的高低會大幅改變分公司帳面上的利潤。若分公司向總公司支付大量資金，分公司的利潤就會減少，連帶地在分公司所在國應繳納的企業所得稅也會隨之減少。報告指出，Palantir 在歐洲各國的子公司編製會計帳簿時，採用將合約產生的收益匯往美國總公司，並僅從美國總公司獲取少量服務手續費作為回報的結構。

在這種結構下，歐洲子公司的帳面利潤被設定得低於實際營業規模。報告表示，西班牙則採用了另一種方式：西班牙子公司將透過公共採購獲取的利潤中的 70% 以技術授權費名義匯給美國總公司，從而大幅減少了西班牙分公司作為課稅對象的利潤。報告更指出，以自家股票代替現金發放給員工的股票報酬制度，也在稅法上被列為費用處理，用來減少應課稅所得。公司若將股票分發給員工，便能在會計帳簿中將該股票的價值反映為人事成本。

由於人事成本在稅法上被認列為費用，這項費用越大，作為課稅對象的利潤就越少。在普遍流行以股票代替現金發放薪資的科技業界，這種方式常被用作合法的節稅手段。

報告亦提出了按國家劃分的數據。CICTAR 推算，由於此類會計結構，2024 年在德國造成的稅源損失高達 160 萬歐元，而同年 Palantir 德國子公司實際繳納的企業所得稅僅為 64 萬歐元。報告提到，在西班牙，Palantir 與國家治安相關機構簽訂了價值 1,650 萬歐元的合約，但實際繳納的企業所得稅僅為 14 萬 7,000 歐元。這些數據均為 CICTAR 分析後提出的結果，並非各國政府的官方公布資料。

在英國則確認了另一個案例。據媒體 Novara Media 於 2026 年 6 月 4 日報導，英國國民保健署（NHS）與 Palantir 簽署了一份價值 3 億 3,000 萬英鎊的整合數據平台合約。該合約被稱為聯邦數據平台，是一項旨在將英格蘭全境的醫院與診療紀錄整合至單一系統的計畫。Palantir 於 2023 年獲選為該計畫的首選應標商，由於這是一份涉及患者敏感醫療資訊的合約，因此自獲選當時起便在英國醫療界與政壇引發爭議。

根據同一報導，帕蘭提爾英國子公司 2024 年向英國稅務機關繳納的公司稅僅為 200 萬英鎊。與 3 億 3000 萬英鎊的合約規模相比，所繳納的公司稅還不到其 165 分之一。當然，將合約總額與單一年度的公司稅繳納額直接進行比較並非精確的計算方式。因為合約總額並非全數認列為當年的利潤，且公司稅是針對利潤而非營業額課徵。然而，這些數字至少凸顯出一個事實：兩者之間的差距極為顯著。

英國下議院科學技術委員會在一份單獨報告中指出，公共部門中帕蘭提爾影響力日益擴大的現狀，是一個難以接受的脆弱點。

將德國、西班牙與英國的案例放在一起審視，便會浮現出一種共同模式。這三個國家雖然都與帕蘭提爾簽署了相當規模的公共合約，但實際徵收到的公司稅相較於合約規模卻極其微小。儘管三國稅務機關以各自不同的方式審查會計帳目，結果卻如出一轍。CICTAR 報告分析指出，這顯示該會計結構可能並非源於特定國家的監管鬆懈，而是源於帕蘭提爾在多國共通採用的會計政策。

CICTAR 報告列為特例的國家是法國。根據報告，法國國稅局要求帕蘭提爾將其在法國境內賺取的利潤完整記錄於法國分公司的帳簿上，結果帕蘭提爾法國分公司在 2024 年以 33% 的實效稅率繳納了 160 萬歐元的公司稅。與其他國家的數據相比，這是高出許多的比例。報告解讀認為，這一差異源於法國國稅局積極的稅務執法。法國同時也是自 2019 年起對在境內創造營業額的大型數位企業課徵獨立數位服務稅的國家。

這項針對美國大型科技企業的稅制，此前曾多次與美國政府引發貿易摩擦。法國國稅局對帕蘭提爾的執法方式，亦可視為此類稅務政策的延伸。

歐盟委員會不僅僅依賴個別成員國的稅務執法，亦在另行推進統一多國企業課稅基準本身的方案。這項稱為 BEFIT 的提案，主張在歐盟內部營運的多國企業不再於各成員國採用不同方式計算稅金，而是依據單一共通標準來計算應課稅所得。該提案目前仍處於歐洲議會與歐盟理事會的審議階段，被認為是從根本上減少 CICTAR 報告所指出的利用移轉定價進行利潤轉移問題的嘗試之一。

該報告出版後，勞工界隨之做出反應。據德國媒體 Labnet Germany 於 2026 年 8 月 5 日報導，國際公共服務工會（PSI）總幹事揚·威萊姆·古德里安（Jan Willem Goudriaan）表示，應停止將國家核心採購委託給未能維護公共衛生與社會安全網預算的海外供應商。同一報導亦引述荷蘭最大工會 FNV 相關人員的發言，指出企業既享用公共基礎設施帶來的便利，卻未繳納相應稅額，這種做法不應再被容忍。發起此類呼籲的團體建議，應將納稅紀錄納入公共採購招標規格書中。

以往公共採購主要以價格與技術性能作為核心評估標準，而該建議則是提議在此基礎上額外納入企業實際繳納的稅額。至於這項建議是否已具體反映於實際採購規定中，在本書所查證的資料範圍內尚無法證實。

這項稅務問題亦與 5.1 節所探討的投資缺口息息相關。EuroStack 報告估算歐洲至 2035 年需籌措 3000 億歐元，而歐盟實際編列的預算則遠低於此。主張稅務改革的一方認為，正如 CICTAR 報告所言，若以帕蘭提爾為首的域外企業能就其在歐洲賺取的利潤繳納相應稅款，該筆稅收便能成為 EuroStack 所需投資資金的一部分。當然，這種因果關係屬於支持 CICTAR 報告一方的政治主張，並非本書另行查證的事實。

這項稅務問題與前章討論的安全問題雖處於不同層面，卻導向了相同的結論。第一章與第四章探討的是將國家的數據與系統運作託付給帕蘭提爾等企業時產生的控制權問題；CICTAR 報告提出的則是，在這些合約中究竟有多少資金實際上能回流至國家財政。義大利國家網絡安全局表示，已綜合考量這兩項因素，確立了在國家核心採購中排除美系平台的政策方向。

稅務與安全這兩個截然不同的依據指向同一個結論的事實，正被舉為歐洲政策制定者無法再推遲處理此一問題的原因。

無論是 EuroStack 所要求的 3000 億歐元、開發 Arcadia 與 openDesk 的費用，還是 CICTAR 所指出的稅源，最終都匯聚為同一個問題：當歐洲試圖建立不依賴美國企業的技術基礎時，建立該基礎的資金從何而來？無論是導引沉睡於銀行中的存款、利用現有預算開發軟體，抑或是堵住滲漏的稅收，這三條途徑皆指向同一個目的地。

從公民的角度來看，這項問題絕非抽象的會計爭論。警察局、醫院與國防部所支付的採購預算均來自市民的稅款。若該預算相當一部分未能透過獲標企業的稅捐重新回流國庫，用於公共服務的資金就會相應減少。CICTAR 與 Follow the Money 所提出問題的核心，正在於這一循環結構當前已經中斷。要讓「繳納稅款、以稅款營運公共服務，再由公共服務支援企業活動」的循環正常運作，必須確立一個前提：獲得採購合約的企業必須在該國繳納其應負擔的相應稅額。

依據與參考文獻

1. Sebastiaan Brommersma, 'Tech giant Palantir accused of aggressive tax avoidance at Europe's expense', Follow the Money, 2026年 8月 5日, https://www.ftm.eu/articles/us-tech-giant-palantir-tax-avoidance-europe

2. Rika Baack, 'Dubiose Praktiken: Palantir drückt sich vor Steuern', netzpolitik.org, 2026年 8月 5日, https://netzpolitik.org/2026/dubiose-praktiken-palantir-drueckt-sich-vor-steuern/

3. Rika Baack, 'Big Data bei der Polizei', LabourNet Germany, 2026年 8月 5日.

4. ITEP, 'Palantir Pays Zero Federal Income Tax Despite Explosive Growth, Largely Due to Trump Tax Law', ITEP Reports, 2026年 3月 22日.

5. Joshua Carroll, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026年6月4日.

6. 英國下議院科學技術委員會, 報告, House of Commons, 2026年.

7. 義大利國家網路安全局, 'Sovranità digitale e IA: l'Italia tra autonomia e dipendenza', 義大利政府, 2026年.

結論 1 替代方案成熟前的宣告，克服未來 2 至 3 年的風險區間

2025 年 12 月 15 日，帕蘭提爾宣布與法國國內安全總局簽署了一份為期 3 年的新多年度合約。然而在這份合約簽署還不到六個月的 2026 年 6 月 16 日，法國總理塞巴斯蒂安·勒科爾尼便宣告將把該合約的合作對象更換為法國企業 ChapsVision。隔天《世界報》報導，帕蘭提爾方面主張續簽的合約在法律上依然有效。宣告與合約終止並非同一件事。本書第一章探討的這一案例，濃縮呈現了歐洲各國政府在未來 2 至 3 年內必須管理的轉型風險究竟呈現何種型態。

必須先檢視採購的問題。法國內政部預估部署新軟體並轉移現有資料需要 18 至 24 個月，而其他報導則認為整個合約結構的完全轉型將耗時於 2027 年至 2029 年之間。內政部長羅朗·紐涅茲表示，為了填補這一空窗期，在 2027 年之前將設立讓帕蘭提爾與 ChapsVision 共同運作的過渡期。相同的問題在德國也在重複發生。

德國聯邦憲法保衛局於 2026 年 5 月確定採購 ArgonOS 來取代帕蘭提爾，但若要這項採購真正投入運作，必須先通過一份重新規定聯邦情報局與聯邦憲法保衛局權限、長達 700 多頁的法律修正案。德國聯邦憲法法院將這項修法的期限設定在 2026 年底。確定採購的事實與該採購實際啟動的時間點，各自被綁定在不同的程序之中。

合約本身的條件有時也會決定轉型的速度。巴登-符騰堡邦內政部於 2025 年 3 月簽署了引進帕蘭提爾 Gotham 系統 integration 的合約，條件是在沒有中途終止條款的情況下，於 5 年內支付 2,500 萬歐元。參與邦聯合政府的綠黨內部對於應立即中止該合約的意見獲得了 92% 的贊成，但缺乏退出條款的合約並未僅憑政治反對就被推翻。這份合約用數字證明了一個事實：若未在採購合約中預先納入解約條件，國家將會自行喪失談判籌碼。

人員與資料遷移的問題發生在合約書之外。法國國內安全總局的人員已經習慣了帕蘭提爾的畫面布局與操作方式，且儲存資訊的方式本身就是按照美國系統的規格來建構的。若要轉用新軟體，必須依序經過多個階段：將現有的操作方式調整適應新介面、重新培訓人員、建立新的資料傳輸路徑、確保進行中的調查不致中斷，以及驗證是否能承受實際的工作量。德國聯邦國防軍也在經歷類似的程序。

網路與情報空間指揮部的托馬斯·達姆海軍中將於 2026 年 4 月表示，已將帕蘭提爾從軍用雲端專案 pCloudBw 的候選名單中排除；此後，德國企業 Almato、柏林新創企業 Oakrist Technologies 以及法國企業 ChapsVision 這三家公司在 2026 年夏季期間進行了連動實戰資料的測試。最終得標者預計將於 2026 年底公布。將帕蘭提爾排除一事與重新遴選何者，目前仍是各自獨立的問題。

荷蘭則面臨著採購碎片化這一另一形式的風險。國防次長戴爾克·博斯維克於 2026 年 6 月 2 日在眾議院表示，將儘快以歐洲替代方案取代帕蘭提爾，並以 2 年內尋得完全同等水準的替代方

案為目標。然而，政府隨後向眾議院提交的答覆中，並未包含具體的終止期限，僅採用了檢討替代案與減少依賴度等字眼。這份答覆背後的原因在於，國防部內部與帕蘭提爾簽署的合約是由各部門獨立進行，甚至缺乏政府層面的統一合約清單。

博斯維克次長本人也承認，若立刻切斷合作關係，可能會在作戰戰鬥系統、國防後勤與情報處理方面產生安全防禦空窗。這等於是荷蘭政府親自證實了宣告的速度與執行的速度大不相同的事實。

在聯合作戰領域，轉型的方向反而朝相反方向發展。北大西洋公約組織於 2025 年宣布，已引進帕蘭提爾的 Maven 智慧系統供盟軍聯合作戰司令部使用。這項引進宣告與 2026 年的現在該系統實際上運作至何種範圍，仍是需要區分看待的問題。不過，正如本書第三章所述，在國內治安情報領域排除帕蘭提爾的舉措，與在軍事同盟領域維持帕蘭提爾地位的趨勢在同一時期並行發生，這一點是無庸置疑的。

歐盟《人工智慧法》第 2 條與前言第 24 項，已將用於軍事、國防及國家安全目的的人工智慧系統排除在規範適用範圍之外。這意味著國內情報機構的退出，並不會自動延伸至國防與北約層面的採購。荷蘭國防部之所以將「若要與北約盟國交換情報就必須使用相同系統」的互通性要求列為轉型的障礙，原因即在於此。此外，美國《雲端法》規定，只要是美國法人處理的資訊，無論伺服器位置為何，皆為美國調查機關開闢了存取管道。在轉型尚未結束的階段，該法律的管轄範圍依然存在。

替代供應商的成熟度同樣決定了這段轉型期的長短。ChapsVision 自 2019 年成立以來，經過 25 起以上的併購，在 2025 年實現了 2 億歐元的營收，但與成立已久的帕蘭提爾相比，仍是一家處於成長階段的公司。德國的最終候選者 Almato 與 Oakrist Technologies 也必須等到 2026 年底才能確定是否投入實戰部署。歐盟執委會提出目標，希望透過《雲端與 AI 法案》，在 5 至 7 年內將歐盟資料中心的容量提升三倍以上，以在 2035 年前滿足企業與公共行政的需求。

這項法案截至 2026 年 8 月仍為執委會提出的規章提案，尚未正式簽署生效。擴充供應能力計畫的完成時間點本身，就已經指向了 2030 年代中期。

Anthropic 於 2026 年 6 月發生的事件構成了這一切轉型的背景。美國政府於 6 月 12 日向 Anthropic 發出出口管制指令，要求切斷外籍人士對 Fable 5 與 Mythos 5 的存取權限。雖然存取權限在出口管制解除後隨之恢復，但該事件實體展示了一種可能性：供應隨時都有可能中斷，而非永久性的封鎖。在法國、德國與荷蘭各自以不同速度尋求替代方案的同時，這種可能性依然未曾消失。

本書所探討的案例中共同展現的一點是：宣告的日期與實際完成轉型的日期之間，無一例外存在著數年的時間差。在填補這段時間差的過程中，各國無法避免同時使用美國技術與歐洲替代方案的雙軌運作。

依據及參考文獻

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

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. 作者不詳, '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. 作者不詳, '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. 作者不詳, '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. Egle Kristopaityte, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

8. 作者不詳, '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-aienabled-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

結論 2 保持開放性的具韌性自立（Resilient Openness）之路

瑞士聯邦公共衛生局、聯邦統計局、聯邦資訊科技局、國防採購局 Armasuisse 以及洗錢防制通報處這五個機構，在 2020 年至 2024 年間的四年間，屢次決定不引進帕蘭提爾（Palantir）。瑞士並不像法國或德國那樣，需要拆除已經導入的程式；而是從一開始阻止其跨過門檻的機構逐漸累積，如今已達到甚至不大需要重新說服的狀態。

資安媒體 ZenData 於 2026 年 2 月報導，瑞士拒絕帕蘭提爾的原因並非性能不足，而是其獨佔且不透明的內部結構、外國的司法管轄權，以及透過遠端進行的更新方式，被評估為無法控制的主權風險。瑞士方面的判斷是，僅憑將資料留在瑞士境內並在合約中加入保護條款，不足以充分防範此一風險。然而，這並不意味著瑞士封鎖了所有的外國技術。

瑞士真正排除的只是帕蘭提爾這一特定供應商，而其判斷標準並非國籍，而是資料的所在地、管轄權以及更新控制權。

西班牙的措施也展現了類似脈絡的選擇。西班牙首相府於 2026 年 7 月 1 日向電信企業 Telefónica、國防企業 Indra、造船企業 Navantia 等國營企業控股公司旗下的公營事業發出指引，指示不得與帕蘭提爾簽訂新合約。但並未將已簽訂的合約廢除。西班牙軍事情報中心與帕蘭提爾簽署的約 1,650 萬歐元規模合約，將持續執行至 2026 年 11 月。這意味著西班牙政府從政策設計階段就承認，阻止新合約與終止既存合約是兩碼子事。而在另一端，則有巴登-符騰堡邦的案例。

這份缺乏退出條款、以 5 年及 2,500 萬歐元綁定的合約，即便在邦聯合政府內部有 92% 的反對票，也無法逆轉。德國聯邦憲法法院亦於 2023 年 2 月裁定黑森邦與漢堡邦將基於帕蘭提爾的系統用於預測性警政的法律依據違憲，認定在缺乏法律依據的情況下廣泛分析公民的通訊紀錄與個人資料，侵害了資訊自我決定權。若合約沒有退出機制，無論是政治意志還是司法機關的判決，都需要時間才能落實為行動。

將這些案例並陳，便能揭示完全封閉與無條件依賴這兩個極端，正以各自的方式瓦解。荷蘭國防次長德克·博斯維克（Derk Boswijk）親自承認的內容，印證了封閉路線的局限。他指出若立即與帕蘭提爾斷絕關係，作戰戰鬥系統、國防後勤與情報處理可能會出現安全真空；同時他也承認，在軍事人工智慧領域，目前尚無同等水準的歐洲替代方案。沒有能力作為後盾的封閉，最終只能停留在宣告層面。

相對地，依賴路線的局限則體現在 2026 年 6 月的 Anthropic 出口管制事件，以及無論伺服器位置為何均允許美國執法機關調閱資料的美國《雲端法案》。僅憑條約或合約中的條文，無法阻止這種曝險。歐盟《人工智慧法案》將用於軍事、國防及國家安全目的的人工智慧系統排除在

適用範圍之外，這也證明了歐盟早已選擇在不同領域採取不同標準，而非在所有領域套用相同規則。

歐盟委員會提出的《雲端與人工智慧發展法》提案，展現了歐洲在這兩個極端之間實際選擇的道路。截至 2026 年 8 月，該法並非已正式頒佈的法律，而是委員會的規章提案；其作為「人工智慧大陸行動計畫」的一環，包含了在 5 至 7 年內將資料中心容量提升至三倍以上，以在 2035 年前滿足企業與公共行政需求的目標。本書第四章探討的四階段主權保證等級設計與以主權為由的解約權條款，正是選擇性地隔離最敏感領域，而在其餘領域繼續採購外國技術，同時預先確保退出合約之權利的方式。

這可以看作是企圖透過制度，預先防止巴登-符騰堡邦所遭遇的無退出機制合約問題。本書第五章討論的法蘭切斯卡·布里亞（Francesca Bria）等人的 Eurostack 構想，亦出自類似的問題意識。該報告指出，重構全歐洲的數位基礎設施需要相當規模的多年度投資。至於確切的總額，仍需根據原報告的詳細項目進一步確認。

這種試圖同時兼顧開放性與自立的作法，目前並非既定的最終成果，而是正在進行中的嘗試。該嘗試究竟有多大成效，取決於未來幾項明確的時間點。德國聯邦國防軍將於 2026 年底決定 pCloudBw 計畫的最終供應商。德國聯邦議院須依照聯邦憲法法院設定的期限，在 2026 年底前通過重新規範情報機關權限的法律。法國內政部承諾在 2027 年前將帕蘭提爾與 ChapsVision 並行運作。西班牙軍事情報中心與帕蘭提爾的合約則將於 2026 年 11 月到期。

這些時間點能否切實遵守，以及填補其缺口的歐洲替代方案能否在實戰中證明具備達到帕蘭提爾水準的穩定性，將是衡量這一既非封閉亦非無條件依賴的折衷方案能否成立的下一個基準。

依據及參考文獻

1. 作者不詳, '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. 作者不詳, '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

5. Egle˙Kristo˙paityte˙, '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

12. 作者不詳, '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

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

金京鎭

kimkj.com