디지털 주권의 이중 구조

유럽의 탈(脫)팔란티어와 아메리칸 빅테크의 사슬

김경진 변호사

서문

이 책은 2026년 8월 11일을 기준으로 유럽의 공공기관과 안보 조직이 미국 소프트웨어, 클라우드, 인공지능 공급자에 기대 온 구조를 검토합니다. 팔란티어를 둘러싼 조달 변화와 유럽연합의 클라우드·AI 개발법(CADA) 제안을 함께 다룹니다.

CADA는 유럽연합 집행위원회가 2026년 6월 3일에 낸 규정 제안입니다. 이 원고를 마친 시점에는 유럽의회와 이사회의 입법 절차가 남아 있습니다. 본문은 공개된 공식 문서, 기업 발표, 의회 자료와 언론 보도를 대조해 구성했습니다.

김경진

목차

제1장. 유럽의 탈(脫)팔란티어와 안보의 자립

1.1. 프랑스 국내보안총국(DGSI)의 결단: 햅스비전(ChapsVision) 아르곤OS로의 전환

프랑스 국내보안총국은 2014년 국내 정보 업무를 다루던 기존 조직을 개편하며 만들어진 기관입니다. 테러 위협을 감시하고 외국의 간첩 활동과 사이버 공격에 대응하는 일이 이 기관의 임무입니다. 국내보안총국은 2016년부터 미국 기업 팔란티어의 데이터 분석 프로그램 고담을 써 왔습니다. 도입의 계기는 2015년 11월 파리에서 일어난 테러 사건이었습니다. 국내보안총국은 테러 조직의 통신 기록과 이동 경로, 자금 흐름을 하나의 화면에서 살펴볼 도구가 급했고, 팔란티어의 프로그램이 그 자리를 채웠습니다.

프랑스 정부가 이 의존을 처음부터 방치한 것은 아닙니다. 내무부는 2021년, 형식이 다른 방대한 데이터를 하나의 국가 체계로 처리할 프랑스 기업의 기술을 찾는 입찰 사업 OTDH를 열었습니다. 이 입찰에는 햅스비전과 함께 방산 대기업 탈레스와 정보기술 기업 에비덴이 함께 세운 합작사 아테아(Athea), 소프트웨어 기업 블루웨이가 뛰어들었습니다. 그러나 어느 후보도 국내보안총국의 일상 업무를 통째로 넘겨받을 만큼 빠르게 자리를 잡지는 못했습니다.

국내보안총국이 2025년 12월에 팔란티어와 다시 손을 잡은 배경에는 이렇게 대체 기술이 아직 현장에 완전히 뿌리내리지 못했다는 현실이 있었습니다.

2025년 12월 15일, 팔란티어는 국내보안총국과 다년 계약을 갱신했다고 발표했습니다. 3년 기한의 계약이었습니다. 계약을 새로 맺은 지 여섯 달이 채 지나지 않은 2026년 6월, 프랑스 정부는 이 계약과 정면으로 부딪히는 결정을 내립니다.

발단은 미국 정부의 조치였습니다. 미국 인공지능 기업 앤트로픽은 2026년 6월 9일 자사의 가장 뛰어난 모델인 페이블 5와 미토스 5를 세상에 내놓았습니다. 그러나 사흘 뒤인 6월 12일 오후 5시 12분(미국 동부시간), 미국 정부는 국가 안보를 이유로 외국 국적자의 페이블 5와 미토스 5 접속을 즉시 중단하라는 수출 통제 지시를 내렸습니다. 사용자의 국적을 빠르게 가려낼 방법이 없었기 때문에, 앤트로픽은 유럽을 포함한 해외 사용자 전체의 접속을 우선 차단하는 쪽을 택했습니다.

막 출시된 최신 모델을 써 보려던 유럽의 연구자와 행정 기관들은 사흘 만에 그 길이 막히는 상황을 겪었습니다. 이 접속 중단은 7월 1일을 전후해 수출 통제가 풀리면서 복구되었지만, 유럽 쪽은 동맹국이 법 하나로 핵심 기술의 접속을 끊을 수 있다는 사실을 눈앞에서 확인했습니다.

이 사건이 나오기 몇 달 앞서, 유럽의회는 이미 기술 의존을 줄이자는 쪽으로 방향을 잡아 두고 있었습니다. 유럽의회는 2026년 1월 22일, 유럽의 기술 주권과 디지털 기반시설에 관한 결의안을 찬성 471표, 반대 68표, 기권 71표로 채택했습니다. 이 결의안은 클라우드 기반시설과 반도체, 인공지능, 사이버 보안 영역에서 소수의 외국 사업자에게 지나치게 의존하는 상황을 우려하고, 공공 조달에서 공개 소프트웨어를 우선하는 원칙과 100억 유로 규모의 주권 기술 기금을 제안했습니다.

프랑스의 결정은 이 결의안이 채택되고 다섯 달 뒤에 나온, 개별 국가 차원의 실행 사례였습니다.

프랑스 정부는 이 사태를 나흘 동안 지켜본 뒤 움직였습니다. 세바스티앙 르코르뉘 총리는 2026년 6월 16일, 국내보안총국이 쓰던 팔란티어의 도구를 프랑스 기업 햅스비전의 아르곤OS로 바꾸겠다고 발표했습니다. 발표 시점은 파리에서 열리는 유럽 최대 기술 전시회 비바테크의 개막 하루 전이었습니다. 하루 앞선 6월 15일에는 햅스비전이 프랑스 혁신 기업 지수인 넥스트40에 이름을 올렸습니다.

넥스트40은 프랑스 정부가 2019년부터 운영해 온 지원 목록으로, 기업 가치가 10억 유로를 넘는 유니콘이거나 3년 안에 1억 유로 넘게 투자를 유치한 기업만 이름을 올릴 수 있습니다. 두 소식이 이틀 사이에 겹치면서, 이 결정이 정부가 오래전부터 준비해 온 그림이라는 인상을 남겼습니다. 르코르뉘 총리는 정보 기술 영역에서 또 다른 전략적 의존을 받아들일 수 없다고 말하고, 우방의 호의에 기대는 시대는 끝났다고 밝혔습니다.

여기서 짚어야 할 사실이 있습니다. 발표와 계약 종료는 같은 사건이 아닙니다. 발표 다음 날인 6월 17일, 르몽드는 팔란티어 쪽이 2025년 12월에 갱신한 계약은 법적으로 여전히 유효하다고 주장한다고 보도했습니다. 프랑스 정부가 새 공급자를 공개적으로 선언한 일과, 기존 계약이 실제로 종료되는 일은 서로 다른 절차를 거쳐야 합니다. 프랑스 내무부도 팔란티어와 맺은 연장 계약의 남은 기간을 인정하면서, 계약을 정리하는 데는 별도의 행정

절차가 필요하다고 밝혔습니다.

실제 교체에는 시간이 더 걸립니다. 프랑스 내무부는 새 프로그램을 정보 현장에 배치하고 기존 데이터를 옮기는 작업에 18개월에서 24개월이 걸릴 것으로 내다봤습니다. 다른 보도는 계약 구조 전체를 놓고 볼 때 완전한 전환이 2027년에서 2029년 사이에 걸쳐 이루어질 것으로 보기도 합니다. 로랑 뉘네즈 내무장관은 이 공백을 메우기 위해 2027년까지 두 체계를 함께 운영하는 과도기를 두겠다고 약속했습니다. 이관이 오래 걸리는 이유는 프로그램 하나를 바꾸는 문제가 아니기 때문입니다.

국내보안총국은 기존에 써 오던 조작 방식을 새 화면에 맞추어 옮기고, 요원들을 다시 교육하고, 데이터가 오가는 경로를 새로 마련하고, 진행 중인 수사가 끊기지 않도록 지켜야 하며, 실제 업무량을 견딜 수 있는지 검증하는 다섯 단계를 순서대로 밟아야 합니다. 국내보안총국의 요원들은 이미 팔란티어의 화면 구성과 조작 방식에 익숙해져 있고, 정보를 저장하는 방식 자체가 미국 시스템의 규격에 맞추어 짜여 있습니다. 연결을 서둘러 끊으면 정보 활동에 공백이 생길 위험이 있어, 프랑스 정부는 단계적인 전환을 선택했습니다.

햅스비전이 개발 중인 새 플랫폼에는 인공지능 에이전트가 검색과 분석의 일부를 대신 수행하는 기능도 들어갈 예정인데, 이 기능이 실제 수사 현장에서 팔란티어의 도구만큼 안정적으로 작동하는지를 확인하는 절차 역시 이관 기간을 늘리는 요인입니다.

이 결정을 뒷받침한 것은 프랑스 2030 투자 계획이었습니다. 정부는 인공지능 영역의 자립을 위해 6억 5,500만 유로를 추가로 배정했습니다. 이 가운데 일부는 공무원용 대화형 인공지능 도구 개발에 쓰였습니다. 2026년 6월 16일, 공직 담당 장관 다비드 아미엘은 그동안 만 명 규모로 시험 운영하던 챗봇 '라시스탕(L'Assistant)'을 백만 명에 이르는 공무원 전체로 넓히겠다고 발표했습니다. 확장의 첫 단계 비용은 70만 유로에서 75만 유로 사이로 집계되었고, 개발은 프랑스 인공지능 기업 미스트랄 AI가 맡았습니다.

미스트랄 AI의 아서 멘치 대표는 유럽이 미국의 클라우드 인프라를 빌려 쓰는 구조를 벗어나 스스로 인프라를 가져야 한다고 말해 왔습니다. 이 발언은 국내보안총국의 결정에 논리적인 뒷받침이 되었습니다.

프랑스의 새 공급자가 된 햅스비전은 2019년 올리비에 델렌바흐 대표가 세운 회사입니다. 델렌바흐 대표는 이전에 금융 분석 소프트웨어 회사 이프론트(eFront)를 2019년 블랙록에 13억 달러에 매각한 경력이 있습니다. 햅스비전은 자체 개발보다 인수를 통해 몸집을 불리는 전략을 택했습니다. 고객관계관리 소프트웨어 기업 코에리스, 소매 데이터 기업 옥티파스, 전자상거래 기업 스파코, 마케팅 자동화 기업 엔피6를 잇달아 사들인 뒤, 사이버 보안과 첩보, 음성 인식 기술을 보유한 베르탱IT와 벡시스까지 인수했습니다.

베르탱IT와 벡시스를 인수하면서 매출은 3천만 유로에서 4천만 유로로, 직원 수는 260명에서 380명으로 늘었습니다. 이런 인수를 스물다섯 건 넘게 반복한 끝에 회사는 프랑스 국책 투자은행 비피프랑스와 티케하우 캐피털의 자금을 받았고, 2022년에는 1억 유로를 추가로 조달했으며, 2025년 한 해 매출은 2억 유로에 이르렀습니다.

햅스비전이 만든 아르곤OS는 형식이 서로 다른 정보를 한데 모아 분석하는 프로그램입니다. 문서뿐 아니라 영상, 음성, 공개된 인터넷 정보를 뜻하는 오픈소스 인텔리전스까지 한곳에서 다룹니다. 이 프로그램은 외부 통신망과 끊어진 에어갭 환경이나, 국가가 직접 관리하는 주권 클라우드 위에서 돌아갑니다. 회사의 지분은 전액 유럽 주주가 쥐고 있습니다. 이 소유 구조가 중요한 이유는 미국의 클라우드법(CLOUD Act) 때문입니다. 이 법은 미국 법인이 운영하는 서비스라면 서버가 어느 나라에 있든 미국 수사기관의 요청에 따라 정보를 내놓아야 한다고 규정합니다.

아르곤OS는 미국 법인이 아니므로 이 법의 적용 범위 밖에 놓입니다.

국내보안총국이 햅스비전을 고른 절차도 살펴볼 필요가 있습니다. 이 회사는 프랑스 내무부가 2021년에 시작한 정보 통합 사업 OTDH의 입찰을 거쳤습니다. OTDH는 형식이 다른 방대한 데이터를 하나의 국가 체계로 처리하려는 사업으로, 전체 예산은 약 4천만 유로로 책정되었습니다. 햅스비전은 3년 넘는 심사 끝에 2024년 말 원천 데이터를 정리하는 1구역(로트1) 사업권을 따냈습니다. 2구역(로트2)을 둘러싼 경쟁은 더 치열했습니다.

이 구역의 마지막 단계에는 탈레스와 에비덴의 합작사 아테아, 소프트웨어 기업 블루웨이, 그리고 햅스비전 세 곳이 남았고, 햅스비전은 2026년 6월에 이 경쟁에서도 이겨 정보를 시각화하고 모델로 만드는 2구역 사업권까지 얻어 최종 낙찰자가 되었습니다. 이 낙찰로

아르곤OS는 국내보안총국을 넘어 여러 사법 기관의 데이터 처리를 맡는 기반 시스템으로 자리 잡았습니다.

프랑스의 이 결정은 이웃 나라에도 영향을 미쳤습니다. 독일 연방헌법수호청은 2026년 5월, 프랑스보다 앞서 같은 아르곤OS를 도입하기로 확정했습니다. 이 결정의 배경과 진행 과정은 다음 절에서 다룹니다.

프랑스 국가 기구 안에서 미국 기술을 완전히 걷어내는 일은 몇 달 안에 끝날 사안이 아닙니다. 요원들의 손에 익은 조작 방식과 데이터 표준, 기존 계약의 남은 기간이 모두 걸림돌로 남아 있습니다. 그럼에도 프랑스 정부가 공개적으로 방향을 바꾼 사실 자체는 뒤집히지 않았습니다. 팔란티어와의 계약이 언제 완전히 끝나는지, 아르곤OS로의 실제 이관이 얼마나 매끄럽게 이루어지는지는 앞으로 확인해야 할 사실로 남아 있습니다.

근거자료

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

10. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 독일 헌법수호청(BfV)의 이탈과 연방국방 클라우드에서의 배제

독일에서는 국내 정보 기관과 군이 각각 다른 시점에, 그러나 같은 방향으로 팔란티어와 거리를 두었습니다. 두 결정은 하나의 사건이 아니라 별개의 절차를 거친 두 개의 사실입니다.

독일 연방헌법수호청(BfV)은 국내 정보를 다루는 최상위 기관입니다. 극단주의 세력의 움직임을 감시하고 외국의 간첩 활동을 막는 일을 맡고 있어, 프랑스의 국내보안총국과 비슷한 위치에 있습니다. 시난 젤렌 청장은 2025년 12월, 독일 내부 회의에서 안보 기관들이 유럽의 관점을 더 뚜렷하게 세워야 하고 장기적인 의존에서 벗어나야 한다고 말했습니다. 이 발언 뒤 다섯 달 만인 2026년 5월, 연방헌법수호청은 팔란티어의 프로그램 대신 프랑스 기업 햅스비전의 아르곤OS를 조달하기로 확정했습니다. 독일 연방 기관이 팔란티어를 공식적으로 거절한 첫 사례로 기록되었습니다.

연방헌법수호청이 고른 아르곤OS는 앞 절에서 설명한 것과 같은 프로그램입니다. 형식이 다른 정보를 통합해 분석하고, 공개된 인터넷 정보를 추적하는 오픈소스 인텔리전스 기능도 갖추고 있습니다. 독일 쪽에서 눈여겨볼 부분은 이 프로그램을 실제로 심는 과정에서 맺은 제휴입니다. 햅스비전은 독일의 경찰 데이터베이스 피아브(PIAV)를 오랫동안 관리해 온 정보기술 회사 로라 시큐리티 솔루션즈와 손을 잡았습니다. 이미 독일 치안망에 자리 잡은 회사와 협력함으로써, 새 프로그램이 기존 체계 위에 무리 없이 얹히도록 한 것입니다.

이 조달이 곧바로 현장에 배치되지는 않습니다. 독일 연방정부는 연방정보국(BND)과 연방헌법수호청의 권한을 새로 정하는 700쪽 넘는 분량의 법률 개정안을 준비하고 있습니다. 이 개정안은 두 기관에 위협 상황에서 직접 개입할 권한과 인공지능, 생체 정보를 다루는 새로운 수단을 부여하고, 연방헌법수호청과 주 정보 기관, 군 방첩 조직인 군사방첩국(MAD) 사이의 정보 공유를 의무화하는 내용을 담고 있습니다. 독일 연방헌법재판소가 이 법 개정의 시한을 2026년 말로 못박아 둔 상태여서, 연방의회는 여름 휴회가 끝난 뒤 곧바로 이 법안을 다루게 됩니다.

아르곤OS를 비롯한 새로운 분석 도구들은 이 법적 틀이 마련되어야 온전히 가동될 수 있습니다. 법이 아직 마련되지 않은 상태에서는 기존 체계를 유지하며 과도기를 보내야

합니다. 조달을 확정한 사실과, 그 조달이 실제로 가동되는 시점은 이렇게 서로 다른 절차에 묶여 있습니다.

연방헌법수호청의 결정과 별개로, 독일 연방군은 군사 영역에서 팔란티어를 배제하는 조치를 따로 밟았습니다. 독일 연방군은 2017년 사이버·정보공간사령부라는 별도 군종을 만들어 사이버 방어와 정보 체계 운용을 전담시켰습니다. 이 사령부의 토마스 다움 해군중장은 2026년 4월 28일, 독일 경제지 한델스블라트와의 인터뷰에서 팔란티어를 군사 클라우드 사업에 쓸 계획이 현재로서는 전혀 없다고 밝혔습니다. 그는 외국 민간 회사 직원에게 독일의 국가 데이터에 접근할 자격을 주는 일은 상상할 수 없다고 말했습니다.

이 발언으로 팔란티어는 연방군이 추진하는 차세대 국방 클라우드 사업 pCloudBw의 후보에서 빠졌습니다. pCloudBw는 부대 곳곳에 흩어진 작전 데이터와 인공지능 처리 능력을 하나의 기밀 클라우드 위에 모으려는 사업으로, 팔란티어가 빠지기 전까지는 검토 대상 후보 가운데 하나였습니다.

이 배제의 배경에는 북대서양조약기구(NATO)와 관련한 우려가 있습니다. NATO는 2025년 3월 팔란티어와 단기 계약을 맺고, 메이븐 스마트 시스템을 지휘 체계에 들였습니다. 메이븐은 위성 영상 정보를 처리하고 타격 표적의 우선순위를 추천하는 프로그램입니다. 그런데 이 프로그램의 일상적인 운용과 관리는 군인이 아니라 팔란티어 소속 민간 기술 인력이 맡고 있습니다. 독일 국방 당국은 전술 정보의 관리 권한을 동맹국의 민간 기업에 맡기는 구조가 국가의 방위 자주권을 해칠 수 있다고 판단했습니다. 여기에 미국 클라우드법(CLOUD Act)도 걸림돌이 되었습니다.

이 법은 미국 법인이 다루는 정보라면 서버 위치와 무관하게 미국 수사 당국이 접근할 길을 열어 둡니다. 독일 연방군의 작전 계획이 이 법의 사정권 안에 놓이는 상황을 국방부는 받아들이기 어렵다고 판단했습니다.

배제 이후 연방군은 대체할 후보를 유럽 안에서 찾았습니다. 다움 중장의 발언이 알려진 2026년 4월 29일 무렵, 연방군은 이미 독일 기업 헬싱의 클라우드·인공지능 체계 알트라와 독일 기업 SAP의 주권 클라우드 체계 S3NS, 프랑스 기업 아토스의 불세쿠아나 XH3000까지 폭넓게 검토하고 있었습니다. 알트라는 이미 일부 연방군 부대에 배치되어 있었고, S3NS는 방산기업 탈레스가 재무와 조달 업무를 옮기는 데 쓰고 있던

체계였습니다. 이렇게 넓게 훑어본 뒤, pCloudBw 사업의 최종 후보는 세 곳으로 좁혀졌습니다.

슈투트가르트에 자리한 알마토(Almato)는 독일 기업 데이터그룹의 자회사로, 독일 연방정보기술보안청(BSI)이 요구하는 기밀 등급 VS-NfD 자료 처리 인증을 갖추고 있습니다. 베를린의 신생 기업 오크리스트 테크놀로지스(Orcrist Technologies)는 형식이 다른 대규모 정보를 하나의 상황 인식 화면으로 묶어내는 기술을 선보였습니다. 파리의 햅스비전도 아르곤OS를 앞세워 이 경쟁에 참여했습니다. 세 회사는 2026년 여름 동안 실전 데이터를 연동하는 시험을 거쳤고, 최종 낙찰자는 2026년 말에 발표될 예정입니다.

팔란티어를 뺀 일과, 누구를 새로 뽑을지는 이렇게 아직 별개로 남은 문제입니다.

팔란티어의 알렉스 카프 대표는 이 결정에 즉각 반응했습니다. 그는 독일 매체 빌트와의 인터뷰에서 이 소식에 놀랐다고 말하고, 독일의 논쟁을 마술에 관한 이야기에 빗대었습니다. 카프 대표는 팔란티어의 기술이 우크라이나 전장에서 이미 검증되었다고 주장하며, 자신과 공동창업자 피터 틸이 독일과 맺어 온 인연을 거론하기도 했습니다. 이에 대해 독일 디지털부 장관 카르스텐 빌트베르거는 외국 기업의 일방적인 통제 아래 놓이지 않는 자립이 국가 안보에서 가장 먼저 지켜야 할 조건이라고 반박했습니다.

독일이 팔란티어에 신중해진 데는 사법부의 판단도 한몫했습니다. 헤센주는 2017년 팔란티어의 고담을 사들여 헤센데이터(hessenDATA)라는 이름으로 운영해 왔습니다. 독일 연방헌법재판소는 2023년 2월 16일, 헤센주와 함부르크주가 예측 치안을 위해 이 체계를 근거로 쓰던 법률 조항에 위헌 판결을 내렸습니다. 재판소는 시민의 통신 기록과 개인정보를 법적 근거 없이 광범위하게 분석하는 방식이 정보 자기결정권을 침해한다고 판단했습니다. 이 판결은 이후 독일 각 주가 팔란티어 기반 체계를 다시 검토하는 계기가 되었습니다.

그러나 모든 주가 같은 방향으로 움직인 것은 아닙니다. 바덴뷔르템베르크주 내무부는 2025년 3월 20일, 녹색당과의 사전 협의 없이 팔란티어의 고담 프로그램 도입 계약을 맺었습니다. 이 계약에는 중도에 끝낼 수 있는 조항이 들어 있지 않았고, 5년 동안 총 2,500만 유로, 연간으로는 약 925만 유로를 지불하는 조건이었습니다. 주 연립정부에

참여한 녹색당 내부에서는 이 계약을 즉시 중단해야 한다는 의견에 92퍼센트가 찬성표를 던졌습니다. 그러나 출구 조항이 없는 계약은 정치적 반대만으로 뒤집히지 않았고, 주정부는 계약을 그대로 이어갔습니다.

이 사례는 조달 계약에 해지 조건을 미리 넣어 두지 않으면 국가가 스스로 협상력을 잃는다는 사실을 보여줍니다.

여기서 짚어 둘 부분이 있습니다. 유럽연합의 인공지능법(AI Act)은 군사, 국방, 국가안보 목적으로 쓰이는 인공지능 시스템을 규정 적용 범위에서 뺍니다. 이 법의 2조와 전문 24항은 그 근거를 회원국이 저마다 지는 국가안보 책임과 군사 활동의 성격에서 찾습니다. 다시 말해 연방헌법수호청과 연방군이 팔란티어를 배제한 결정은 유럽연합 차원의 인공지능 규제를 따른 결과가 아니라, 독일이라는 개별 국가가 조달과 정치의 영역에서 스스로 내린 선택입니다.

연방 기관과 주 정부의 이 엇갈린 행보는 같은 나라 안에서도 주권을 지키는 속도와 방식이 다르다는 사실을 드러냅니다. 연방헌법수호청과 연방군은 계약을 맺기 전 단계에서 팔란티어를 배제했지만, 바덴뷔르템베르크주는 이미 서명한 계약에 발이 묶여 있습니다.

근거자료

1. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, 'Geheimdienstreform: Zeitenwende für Spione', netzpolitik.org, 2026, https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/

10. 저자 미상, '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. 네덜란드 국방부의 2년 내 전면 대체 전략과 스위스의 철저한 거부 전선

네덜란드와 스위스는 프랑스, 독일과는 다른 모습으로 팔란티어와 거리를 두었습니다. 네덜란드는 이미 쓰고 있는 프로그램을 계획적으로 걷어내려 하고, 스위스는 애초에 팔란티어를 들이지 않는 쪽을 몇 년째 반복해서 선택해 왔습니다.

네덜란드 국방부를 둘러싼 논의는 탐사보도 매체 팔로우 더 머니가 국방부 특수작전사령부(SOCOM)도 팔란티어를 쓰고 있으며, 군사 작전이 진행되는 동안 팔란티어 쪽이 민감한 정보에 접근할 수 있다는 사실을 알리면서 불붙었습니다. 팔로우 더 머니는 앞선 취재에서 네덜란드 군과 경찰이 몇 년째 팔란티어와 은밀하게 거래해 왔다는 사실도 밝힌 바 있습니다. 국방부 쪽은 팔란티어 직원의 접근이 예외적인 경우에 한정되고, 감독 아래 혼자 작업하지 않으며, 실제 기밀 정보가 아니라 가상이거나 오래된 자료만 다룬다고 해명했습니다.

그러나 외국 기업 직원이 어떤 형태로든 비밀 정보에 접근한다는 사실 자체가 국가 안보에 직접적인 위험이라는 지적은 가라앉지 않았습니다. 국방차관 데르크 보스베이크는 이 보도가 나오고 한 달 전인 2026년 5월, 팔란티어 사용을 줄이라는 지시를 이미 부처 안에 내려둔 상태였다고 밝혔습니다. 그는 팔란티어에 대한 의존이 우려스럽다는 점을 인정하면서, 유럽산 대안을 찾으라고 지시했다고 말했습니다. 이 사안이 논란이 된 또 다른 이유는 팔란티어가 인공지능으로 공격 표적을 골라내는 기능까지 제공한다는 점이었습니다.

보스베이크 차관은 2026년 6월 2일 하원(Tweede Kamer)에서 팔란티어를 유럽산 대안으로 되도록 빨리 바꾸겠다고 공식적으로 밝혔습니다. 그는 완전히 동등한 수준의 대안을 찾는 데 2년을 목표로 잡고 있다고 말하면서도, 군사용 인공지능 분야에서는 지금 같은 수준의 유럽 대안이 없다고 인정했습니다. 그는 또 지금 당장 관계를 끊으면 작전 전투 체계와 국방 병참, 정보 처리에 제한적이라도 안보 공백이 생길 수 있다고 밝혀, 즉각적인 단절에는 선을 그었습니다.

발표 이후 실제 진행 상황을 들여다보면 속도는 더디다는 평가가 나옵니다. 정부가 하원에 낸 후속 답변에는 구체적인 종료 시한 대신 '대체안 검토'와 '의존도 축소'라는 표현만

담겼습니다. 진행이 더딘 데는 몇 가지 이유가 있습니다. 국방부 안에서 팔란티어와 맺은 계약이 부처별로 따로 이루어져 있어, 정부 차원에서 통일된 계약 목록조차 없습니다. 진행 중이거나 예정되었거나 이미 끝난 계약을 한눈에 모아 볼 방법이 없다는 뜻입니다. 여기에 군 부대가 NATO 동맹국과 정보를 주고받으려면 같은 체계를 써야 한다는 상호운용성 요건도 걸림돌로 작용합니다.

국경 관리를 맡는 왕립 마레쇼세(Marechaussee)도 국경 감시 시스템에 팔란티어의 도구를 쓰고 있어, 국방부 한 곳의 결정만으로 정리되지 않는 문제이기도 합니다. 정치적으로는 방향을 정했지만, 이를 실행에 옮길 구체적인 동력은 아직 약하다는 것이 이 사안을 취재해 온 매체들의 공통된 평가입니다.

스위스는 이와 결이 다른 사례입니다. 프랑스나 독일처럼 이미 도입한 프로그램을 걷어내는 것이 아니라, 여러 정부 기관이 몇 년에 걸쳐 팔란티어를 받아들이지 않기로 거듭 결정해 온 쪽에 가깝습니다.

스위스 연방보건청은 2020년 4월에서 5월 사이, 코로나19 백신 물류를 관리하는 입찰에 참여한 팔란티어를 걸러냈습니다. 구체적인 사유는 공개되지 않았지만, 담당 부서가 팔란티어의 참여 자체를 문제로 삼았다고 전해집니다. 같은 해 스위스 연방통계청은 팔란티어 쪽의 면담 요청에 응하지 않았습니다. 스위스 연방정보기술청은 2020년과 2021년 사이 팔란티어와 세 차례 회의를 진행한 뒤, 도입할 필요가 없다는 결론을 냈습니다. 스위스 국방조달청 아르마수이스는 2020년, 군 정보국의 정보기술 체계를 위한 입찰에 참여한 팔란티어를 탈락시켰습니다.

탈락 사유는 의무 요건을 채우지 못했다는 것이었고, 그 요건이 무엇이었는지는 공개되지 않았습니다.

2022년 10월에는 스위스 자금세탁방지신고사무국(MROS)이 팔란티어의 소프트웨어 시연을 받았지만, 이를 도입할 법적 근거가 없어 위법 소지가 있다고 판단해 도입하지 않았습니다. 이 흐름은 2024년까지 이어졌습니다. 팔란티어의 유럽 사업 책임자 루이스 모즐리는 2024년 6월 싱가포르에서 열린 안보 회의 샹그릴라 대화에서 스위스 군참모총장 토마스 쥐슬리를 직접 만나 제품을 소개했습니다.

모즐리는 데이터에 인공지능이나 알고리즘을 적용하는 문제에 스위스 군이 관심이 있다는 점을 짚으며, 군 부대의 가동 태세를 측정하는 응용 프로그램을 포함해 제품을 실제로 시연하겠다고 제안했습니다. 스위스 군 참모부는 이 제안을 받은 뒤 내부 검토 보고서를 작성해 2024년 12월 초 쥐슬리 참모총장에게 직접 보고했습니다. 보고서는 팔란티어의 도구를 도입할 경우 스위스 군의 기밀 정보가 미국 중앙정보국(CIA)과 국가안보국(NSA)에 넘어갈 수 있다는 우려를 담았고, 스위스 군은 이 보고를 근거로 도입 계획을 최종적으로 접었습니다.

다섯 개 기관, 네 해에 걸친 거절이 쌓이면서, 스위스에서는 팔란티어를 받아들이지 않는 태도가 하나의 기관 문화처럼 자리 잡았습니다. 팔란티어는 이 기간 내내 스위스 관공서 문을 적극적으로 두드렸지만, 결국 단 한 건의 계약도 따내지 못했습니다. 보안 매체 젠데이터가 2026년 2월 14일 보도한 바에 따르면, 스위스가 팔란티어를 물리친 이유는 성능이 부족해서가 아니었습니다. 독점적이고 불투명한 내부 구조, 외국의 사법 관할권, 원격으로 이루어지는 업데이트 방식이 통제할 수 없는 주권 위험으로 평가되었습니다.

데이터를 스위스 안에 두고 계약서에 보호 조항을 넣는 정도로는 이 위험을 충분히 막을 수 없다는 것이 스위스 쪽의 판단이었습니다.

팔란티어는 이 거절의 흐름을 다루는 언론 보도에도 강하게 반응했습니다. 스위스 탐사보도 매체 리퍼블릭은 2024년 12월, 팔란티어와 스위스의 관계가 위험할 수 있다는 기사 두 편을 냈습니다. 팔란티어는 이 보도에 반박문 스물세 건을 게재하라며 리퍼블릭을 상대로 소송을 걸었습니다. 취리히 상업법원은 스물세 건 가운데 단 한 건의 게재만 인정했고, 팔란티어에 지급하도록 정해진 손해배상액도 9,000스위스프랑 수준에 그쳤습니다. 이 판결은 스위스에서 팔란티어의 신뢰도에 또 하나의 흠집을 냈습니다.

비슷한 시기 스페인에서도 새로운 조치가 나왔습니다. 스페인 총리실은 국영기업지주회사(SEPI) 산하 공기업들에 팔란티어와 새로 계약하지 말라는 지침을 내렸고, 이 소식은 2026년 7월 1일 스페인 언론을 통해 알려졌습니다. 이 조치는 통신기업 텔레포니카, 방산기업 인드라, 조선기업 나반티아처럼 고급 통신망과 군사 정보를 다루는 국영기업들을 겨냥했습니다. 다만 이미 맺은 계약까지 무효로 하지는 않았습니다. 스페인군 정보센터(CIFAS)가 팔란티어와 맺은 약 1,650만 유로 규모의 계약은 2026년 11월까지

그대로 이어집니다.

새 계약을 막는 것과 기존 계약을 끊는 것이 다른 문제라는 사실은 스페인의 사례에서도 똑같이 확인됩니다.

네덜란드와 스위스, 스페인을 나란히 놓고 보면, 유럽이 팔란티어와 거리를 두는 방식이 하나가 아니라는 사실이 드러납니다. 네덜란드는 이미 국방 체계 곳곳에 스며든 프로그램을 정치적 의지만으로는 쉽게 걷어내지 못하고 있습니다. 스위스는 애초에 문턱을 넘지 못하게 막아 온 여러 기관의 판단이 쌓여, 지금은 새로 설득할 필요조차 크지 않은 상태에 이르렀습니다. 스페인은 앞으로 맺을 계약의 문을 닫으면서도 이미 서명한 계약의 만기까지는 그대로 기다리는 길을 택했습니다.

어느 쪽이든, 미국 기술에 기대지 않고 안보 체계를 운영하려면 계약서의 조항 하나, 기관 간의 협의 하나까지 미리 갖추어 두어야 한다는 사실은 같습니다.

근거자료

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

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

3. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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

제2장. 가상에서 현실로: 미국의 킬 스위치 제재 충격

2.1. 앤트로픽 '페이블 5(Fable 5)' 차단 사건과 동맹의 경고

미국 국방부와 인공지능 기업 앤트로픽 사이의 마찰은 2026년 이전부터 조용히 쌓여 있었습니다. 앤트로픽은 정부 기관에 자사의 인공지능 모델을 제공할 때 두 가지 선을 스스로 그어 두었습니다. 하나는 자사의 모델이 사람을 직접 겨냥해 살상하는 무기 체계에 탑재되지 않아야 한다는 것이었습니다. 다른 하나는 자국 시민을 대상으로 한 무차별 비밀 감시 업무에 모델이 쓰이지 않아야 한다는 것이었습니다. 이 두 조건은 회사가 정부와 계약을 맺기 전부터 밝혀 온 사용 정책의 연장선에 있었습니다. 국방부 수뇌부는 이 조건을 받아들이지 않았습니다.

그들은 어떤 제약도 걸리지 않은 완전한 접근 권한을 요구했습니다. 인공지능 모델을 무기 표적 선정 체계에 그대로 연결하거나, 자국 시민의 통신과 위치 정보를 걸러내는 감시 체계에 제한 없이 붙일 수 있어야 한다는 것이 국방부 쪽 요구의 실질적인 내용이었습니다. 앤트로픽은 이런 요구를 받아들이면 자사의 인공지능이 사람의 생사를 가르는 결정이나 자국민에 대한 전면 감시에 직접 관여하게 된다고 보았습니다. 회사는 정부 고객을 잃는 위험을 감수하더라도 이 두 선만큼은 지키겠다는 입장을 고수했습니다. 협상은 좁혀지지 않았습니다.[1]

국방부는 앤트로픽이 물러서지 않자 이 회사를 자국 소프트웨어 공급망의 위협 요소로 지목했습니다. 국방부 관리들은 앤트로픽을 국가 안보에 치명적인 공급망 리스크 기업으로 정식 규정했습니다. 이 지정은 그전까지 미국에 적대적인 국가의 법인에만 내려지던 강도 높은 행정 조치였습니다. 민간 인공지능 기업이 이런 지정을 받은 일은 그때까지 드물었습니다.

트럼프 행정부는 2026년 2월 28일에 연방 정부 기관들이 앤트로픽의 인공지능 프로그램을 쓰지 못하도록 명령했습니다.[1] 이 명령은 겉으로는 조달 규정을 다루는 행정 조치처럼 보였지만, 실제로는 국방부가 원하는 접근 조건을 앤트로픽이 받아들이도록 압박하는 수단이었습니다. 공급망 리스크 기업이라는 지정은 이름만 무거운 표현이 아니었습니다. 이 지정을 받은 법인은 국방부 조달 체계 안에서 신뢰할 수 없는 공급자로 관리되며, 새로운 계약을 맺기가 어려워지고 기존 계약도 재검토 대상에 오르는 것이 일반적이었습니다.

그전까지 이 조치는 미국에 적대적인 국가와 연결된 법인을 걸러내는 용도로 쓰였습니다. 실리콘밸리에서 세계적으로 이름이 알려진 인공지능 개발사가 이 명단에 오른 일은 그때까지 없었습니다. 앤트로픽이 이 지정을 받았다는 사실 자체가, 국방부가 이 갈등을 계약 조건을 둘러싼 협상이 아니라 안보 위협의 문제로 다루고 있음을 보여 주었습니다.

이 압박에 맞서 앤트로픽은 물러서지 않았고, 사안은 법정으로 넘어갔습니다. 연방 법원 판사는 2026년 3월 27일에 국방부의 손을 들어주지 않았습니다. 판사는 국방부가 앤트로픽에 가한 압박이 헌법 수정조항 제1조가 보장하는 표현의 자유를 침해한 정치적 보복이라고 판단했습니다.[1] 민간 기업이 스스로 정한 사용 조건을 지키려다 공공 권력과 정면으로 부딪치고, 그 부딪침이 법원의 판단으로 이어진 사건이었습니다. 이 판결은 미국 안에서는 견제 장치가 작동했다는 사실을 보여 주었습니다.

행정부가 민간 기업에 가한 압박이 부당하다고 판단되면, 사법부가 이를 막아설 수 있었습니다. 하지만 이 사법적 견제는 미국이라는 나라 안에서만 유효했습니다. 이 시점까지는 미국 안에서 벌어진 행정부와 민간 기업 사이의 다툼이었고, 유럽의 정부나 기관은 이 다툼의 결과를 지켜볼 방법도, 그 결과에 개입할 방법도 갖고 있지 않았습니다.

이 내부 갈등은 국내 소송으로 끝나지 않았습니다. 미국 상무부는 2026년 6월 12일에 인공지능 기술의 수출을 제한하는 명령을 내렸습니다. 상무부는 이 조치의 근거로 최상위 수준의 국가 안보 보존을 들었습니다.[2][3] 이 명령이 명시적으로 겨냥한 대상은 외국 국적을 가진 사용자의 접근이었습니다.[2] 그런데 앤트로픽은 접속자의 국적을 실시간으로 가려내는 필터 체계를 갖추고 있지 않았습니다. 인터넷을 통해 서비스를 제공하는 회사가 계정을 등록한 나라나 결제에 쓰인 카드의 발급국은 알 수 있어도, 접속하는 사람 한 명 한 명의 국적을 즉시 확인하기는 쉽지 않습니다.

그래서 앤트로픽은 자사가 보유한 가장 성능이 뛰어난 모델인 클로드 페이블 5와 클로드 미토스 5의 해외 인터넷 접속을 통째로 멈추는 방법을 택했습니다. 명령서가 전달된 지 몇 시간 만에 유럽을 포함한 모든 국외 컴퓨터의 접속이 끊겼습니다.[1][5] 정부의 지시는 외국 국적자를 겨냥했지만, 실제로 끊긴 것은 국적과 무관한 해외의 모든 접속이었습니다. 이번 조치는 미국이 특정 기업이나 개인을 영구히 거래 금지 명단에 올리는 제재와는 성격이 달랐습니다.

상무부가 쓴 수단은 특정 기술의 수출을 국가 안보 사유로 잠시 제한하는 명령이었고, 이런 명령은 법적으로 처음부터 기간이 정해지지 않은 채 발동되더라도 정책 판단에 따라 언제든 거둘 수 있는 성격을 지니고 있었습니다. 다만 유럽의 이용 기관 입장에서는 그 성격의 차이를 알았다고 해서 접속이 끊긴 순간의 충격이 줄어들지는 않았습니다.

유럽의 여러 행정청과 연구소는 사전 경고를 받지 못한 채 매일 쓰던 인공지능 소프트웨어를 잃었습니다.[1][5] 접속이 끊긴 이유를 알리는 공지도, 이의를 제기할 창구도 마련되어 있지 않았습니다. 계약서에 서명하고 이용료를 내 온 기관이라 해도 사정은 다르지 않았습니다. 서비스를 계속 받을 권리는 이용 계약이 아니라 공급자 본국 정부의 수출 통제 판단 앞에서 아무런 힘을 갖지 못했습니다. 클라우드 서비스 약관이나 서비스 수준 협약은 이런 종류의 국가 행정 조치를 막아 주는 장치가 아니었습니다.

유럽의 보안 분야 매체들은 이 사태를 두고 '페이블 밴(Fable-Ban)'이라는 이름을 붙여 다루었습니다. 우방국의 행정 명령 하나가 아무런 사전 협의 없이 동맹국의 업무망을 정지시킬 수 있다는 사실이 취재의 초점이었습니다.[5]

접속을 잃은 쪽은 정부 부처만이 아니었습니다. 유럽 각국의 행정 기관과 함께 대학, 국책 연구소도 일상 업무에 페이블 5와 미토스 5를 쓰고 있었고, 이 기관들 역시 같은 순간에 같은 방식으로 도구를 잃었습니다.[8] 공공 부문과 학술 연구 부문이 함께 겪은 이 단절은, 이번 사태가 특정 부처나 특정 계약 관계에 국한된 문제가 아니라 미국 기술에 의존하는 유럽의 모든 사용자층에 걸친 문제라는 인식을 넓히는 계기가 되었습니다.[8] 독일의 보안 분야 매체 시큐어클라우드 블로그는 미국 소프트웨어가 무기처럼 쓰일 수 있다는 제목의 글에서, 팔란티어를 둘러싼 논란과 페이블 5 차단을 함께 다루며 유럽에 필요한 것은 개별 기업에 대한 불신이 아니라 디지털 주권이라는 결론을 내놓았습니다.[5] 계약을 어느 회사와 맺든, 그 회사의 본사가 미국에 있는 한 같은 위험에서 완전히 벗어나기 어렵다는 지적이었습니다.[5]

이 차단은 18일 동안 이어졌습니다. 미국 정부는 2026년 7월 1일에 이르러서야 수출 제한 조치를 거두었습니다.[3] 앤트로픽은 통제가 풀린 뒤 접근을 되돌리는 절차에 들어갔다고 밝혔습니다.[4] 회사의 설명에 따르면 6월 12일의 조치로 끊겼던 접근은 통제 해제와 함께 곧바로 완전히 복구된 것이 아니라, 복구가 진행되는 방식으로 이어졌습니다.[4] 정책이

뒤집힌다고 해서 서비스가 그 순간 다시 켜지는 것은 아니었습니다. 끊어진 접속을 다시 세우는 데에도 시간이 걸렸습니다. 차단은 명령서가 전달된 지 몇 시간 만에 이루어졌지만, 복구는 그렇게 빠르지 않았습니다.

완전히 이전과 같은 상태로 되돌아오기까지는 시일이 더 필요했습니다. 그럼에도 사건의 결말은 분명했습니다. 접속은 끊겼고, 그리고 다시 열렸습니다.

여기에서 확인해야 할 사실은 두 가지입니다. 첫째, 페이블 5와 미토스 5의 해외 접속은 실제로 끊겼습니다. 유럽의 여러 정부 기관과 연구소가 18일 동안 이 도구 없이 일해야 했습니다. 둘째, 그 차단은 영구히 이어지지 않았습니다. 미국 정부는 정책을 바꾸었고, 접속은 열렸습니다. 이 사건을 미국 인공지능 기술이 유럽에 다시는 공급되지 않는다는 증거로 읽는 것은 사실과 다릅니다. 앤트로픽은 사건 이후에도 유럽에서 영업을 이어 갔고, 유럽의 기관들도 다시 계약을 맺거나 기존 계약을 이어 갔습니다.

반대로 이 사건을 아무 일도 아니었다는 듯 넘기는 것도 사실과 다릅니다. 18일 동안 실제로 벌어진 단절은 되돌릴 수 없는 손실을 남기지는 않았지만, 그 18일 동안 접속이 필요했던 기관들은 대안을 찾거나 업무를 미루는 수밖에 없었습니다. 페이블 5 사건이 실제로 보여준 것은 공급이 언제든 멈출 수 있고, 그 멈춤과 재개를 결정하는 권한이 이용하는 나라가 아니라 공급하는 회사의 본국 정부에 있다는 구조였습니다. 이 사건을 촉발한 갈등은 처음부터 유럽을 겨냥해 시작된 것이 아니었습니다.

국방부와 앤트로픽의 다툼은 미국 안에서 벌어진 조달 협상의 연장이었고, 유럽은 그 협상과 아무런 관련이 없었습니다. 그런데도 유럽의 정부와 연구소는 협상의 결과를 함께 떠안았습니다. 자신과 무관한 분쟁의 여파로 업무 도구가 끊길 수 있다는 사실은, 관련 당사국이었을 때보다 오히려 더 큰 불안을 남겼습니다. 다음에 같은 방식으로 접속이 끊기는 계기가 무엇일지, 유럽의 정부와 기관은 예측할 방법이 없었습니다.

이 구조는 그전까지 유럽의 정책 결정자들에게 손에 잡히지 않는 개념이었습니다. 디지털 주권이라는 말은 학술 세미나의 발표문이나 정책 보고서의 서문에서나 등장하는 표현이었습니다.[1] 우방국 정부가 자국의 국내 정치 다툼을 해결하는 과정에서 내린 수출 통제 명령 하나가, 몇 시간 만에 동맹국 정부 기관의 업무 도구를 정지시킬 수 있다는 사실은 이론이 아니라 실제로 일어난 일이 되었습니다.[1][5] 상무부의 명령이 겨냥한 표적은 외국

국적자였지만, 그 결과로 함께 끊긴 것은 동맹국 정부와 연구소의 접속이었습니다.

이 표적과 결과 사이의 어긋남이 유럽 쪽에서 이 사건을 특별한 경고로 받아들인 이유였습니다. 미국이 유럽을 겨냥해 조치를 내린 것이 아니었는데도, 유럽이 그 조치의 사정권 안에 함께 들어가 있었다는 사실 자체가 문제였습니다. 미국의 수출 통제는 보통 적대 국가로 향하는 기술 유출을 막으려는 목적으로 쓰이는 수단이었고, 북대서양조약기구 회원국을 비롯한 우방국은 그 대상에서 관례적으로 구분되어 왔습니다. 그러나 페이블 5 사건에서는 이런 구분이 실제로는 지켜지지 않았습니다.

우방과 비우방을 가르는 경계는 정책의 의도 안에서만 존재했을 뿐, 국적을 걸러내는 기술적 장치로는 뒷받침되지 않았습니다. 유럽의 정부들이 이 사건에서 읽어 낸 것은 바로 이 간극이었습니다. 의도상의 구분과 실제 집행 사이에 벌어진 틈이, 동맹국이라는 지위만으로는 메워지지 않는다는 사실이었습니다.

가장 빠르게 움직인 나라는 프랑스였습니다. 프랑스 내무장관 세바스티앙 르코르뉘는 상무부의 수출 통제 명령이 내려진 지 나흘 뒤인 2026년 6월 16일에 국내보안총국의 정보 분석 체계를 미국 팔란티어의 프로그램에서 프랑스 기업 햅스비전이 만든 아르곤OS로 바꾸겠다고 발표했습니다.[6] 이 발표를 팔란티어와의 계약이 그 자리에서 끝났다는 뜻으로 읽어서는 안 됩니다. 팔란티어와 프랑스 정부 사이의 계약은 그 시점에도 여러 해가 남아 있었고, 계약을 끝내려면 위약금과 별도의 협상이 뒤따라야 했습니다.

실제 시스템 교체 역시 발표 이후에 진행되는 별도의 과정이었습니다.[7] 그럼에도 프랑스 정부가 상무부의 명령 이후 나흘 만에 이런 방향의 발표를 내놓았다는 사실은, 페이블 5 차단이 유럽의 정부 안에서 얼마나 빠르게 정책 논의로 옮겨 갔는지를 보여 줍니다. 프랑스는 이 흐름에서 가장 먼저 발표를 내놓은 나라였을 뿐, 유일한 나라는 아니었습니다.

페이블 5 차단 이후 몇 달 사이 유럽의 다른 정부들에서도 미국 기술에 대한 의존도를 다시 점검하는 절차가 잇따라 시작되었습니다.[8] 각 나라가 구체적으로 어떤 경로를 밟았는지는 나라마다 달랐지만, 그 출발점에 이번 사건이 있었다는 사실은 공통적이었습니다.

앤트로픽의 사례가 유럽에 남긴 교훈은 회사 하나를 믿을 수 없다는 것이 아니었습니다. 앤트로픽은 국방부의 요구에 맞서 자사가 정한 사용 조건을 지켰고, 법원도 이 회사의 손을

들어주었습니다. 회사가 살상 무기와 무차별 감시라는 두 선을 지키려다 겪은 압박은, 오히려 이 회사가 자신이 정한 원칙에 충실했다는 사실을 보여 주었습니다. 문제로 지목된 것은 앤트로픽의 태도가 아니라, 미국 정부가 마음만 먹으면 어느 미국 기업의 해외 서비스도 같은 방식으로 멈출 수 있다는 구조 자체였습니다.

오늘은 국방부와 앤트로픽 사이의 갈등이었지만, 다음에는 다른 회사와 다른 갈등이 같은 결과를 낳을 수 있었습니다. 그 갈등이 무역 분쟁에서 비롯되든, 안보 정책에서 비롯되든, 아니면 이번처럼 정부와 기업 사이의 내부 협상에서 비롯되든 마찬가지였습니다. 유럽의 정부와 연구소는 그 갈등의 당사자가 아니면서도 결과를 그대로 떠안는 쪽에 서 있었습니다.

18일이라는 시간은 실제 업무가 멈추기에는 짧지 않은 기간이었습니다. 동시에 이 기간이 언젠가 끝난다는 사실도 이번 사건으로 확인되었습니다. 미국 정부의 판단이 바뀌면 접속은 다시 열렸습니다. 유럽의 여러 정부가 이 사건 이후 자국의 기술 조달 정책을 다시 들여다보기 시작한 이유는 바로 이 지점에 있었습니다. 계약서에 아무리 상세한 조항을 담아도, 공급자 본국 정부의 결정 앞에서는 그 조항이 힘을 갖지 못한다는 사실이 이 사건으로 분명해졌습니다. 접속이 끊겼다는 사실보다, 접속의 시작과 끝을 결정하는 권한이 자신들의 손 밖에 있다는 사실이 더 오래 남는 문제였습니다.

페이블 5 사건은 그래서 봉쇄가 영원히 이어졌다는 이야기가 아니라, 봉쇄가 언제든 다시 일어날 수 있고 그 결정권이 다른 나라 정부에 있다는 이야기로 유럽의 정책 문서에 남았습니다. 접속이 복구된 뒤에도 이 사건이 계속 인용되는 이유가 여기에 있습니다. 위기가 지나간 뒤에 남는 질문은 무엇이 끊겼느냐가 아니라, 다음에도 같은 결정을 다른 나라 정부가 내릴 수 있느냐는 것이었습니다. 이 질문에 대한 답을 유럽이 스스로 통제할 수 없는 한, 18일간의 차단은 한 번으로 끝난 사고가 아니라 되풀이될 수 있는 가능성으로 남습니다.

근거자료

1. Centre for Future Generations, 'Enforcement spotlight, Spring 2026', Centre for Future Generations, 2026년 봄호.

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

4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026년, 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, 2026년 6월 8일, 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, 2026년 6월 16일, 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, 2026년 6월 17일, 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. 「유럽연합(EU) 주요국의 탈(脫)팔란티어 행보와 디지털 주권화에 관한 분석 보고서」, 2026년, 1-2쪽.

2.2. 역외 입법의 덫: 미국 CLOUD Act와 FISA 702조 사법 사정권의 실체

유럽연합 회원국들은 오랫동안 데이터 서버를 자국 영토 안에 두면 정보가 안전해진다고 믿어 왔습니다. 아마존과 마이크로소프트, 구글 같은 미국계 기업들도 프랑크푸르트나 파리, 더블린에 데이터센터를 지어 놓고 이 믿음을 광고 문구로 삼았습니다. 그러나 서버가 유럽 땅에 서 있다는 사실과 그 서버 안의 정보가 미국 법의 손이 닿지 않는 곳에 있다는 사실은 서로 다른 이야기입니다. 미국 의회가 만든 두 개의 법, 클라우드법과 해외정보감시법 제702조는 국경이 아니라 회사의 소속을 기준으로 작동하기 때문입니다.

이 두 법이 왜 지금 유럽의 조달 담당자들을 긴장시키는지 이해하려면 먼저 클라우드법이 태어난 배경을 봐야 합니다. 이천십삼년 십이월 미국 연방 수사기관은 마약 거래 수사와 관련해 마이크로소프트에 한 이용자의 이메일 계정 정보를 넘기라는 영장을 보냈습니다. 문제는 그 계정의 데이터가 아일랜드 더블린에 있는 서버에 저장되어 있었다는 점입니다. 마이크로소프트는 미국 영장이 미국 영토 밖의 데이터에는 미치지 않는다며 소송을 제기했고, 이천십육년 뉴욕 연방 항소법원은 마이크로소프트의 손을 들어 주었습니다.

미국 법무부가 이 판결에 불복해 연방대법원까지 사건을 끌고 가는 사이, 미국 의회는 이천십팔년 삼월 이십삼일 클라우드법을 통과시켜 버렸습니다. 새 법이 이 다툼의 근거 자체를 바꾸어 놓았기 때문에 대법원은 사건을 더 심리할 필요가 없다고 판단하고 소송을 종결시켰습니다. 클라우드법은 이렇게 미국 정부가 재판에서 질 뻔했던 다툼을 입법으로 정리하며 태어난 법입니다.

법의 핵심은 간단합니다. 데이터가 어느 나라에 저장되어 있는지를 묻지 않습니다. 그 데이터를 관리하는 회사가 미국의 사법 관할 안에 있는지를 묻습니다. 법률 용어로는 이를 점유, 보관, 통제라는 세 가지 기준으로 표현합니다. 미국에 본사를 둔 회사이거나 미국 회사가 지분과 경영권을 쥔 해외 자회사라면, 그 회사가 점유하거나 보관하거나 통제하는 정보는 저장된 물리적 위치와 관계없이 미국 법원의 영장이나 명령서에 따라 제출해야 합니다.

이 지점에서 클라우드법이 실제로 가능하게 하는 일과, 사람들이 흔히 오해하는 일을 나누어 볼 필요가 있습니다. 클라우드법이 가능하게 하는 일은 분명합니다. 미국 사법 관할

아래 있는 통신 서비스 제공자나 원격 컴퓨팅 서비스 제공자는, 자신이 점유하거나 보관하거나 통제하는 정보라면 그것이 세계 어느 나라 서버에 있든 미국 정부의 적법한 요구에 응해 제출할 법적 의무를 집니다. 반면 클라우드법이 자동으로 뜻하지 않는 일도 여럿입니다. 첫째, 이 법은 미국 정부가 이미 모든 데이터를 손에 쥐고 있다는 뜻이 아닙니다.

정부는 여전히 개별 사건마다 법원의 영장이나 검찰의 소환장 같은 정식 법적 절차를 거쳐야 합니다. 둘째, 모든 요구가 자동으로 관철된다는 뜻도 아닙니다. 클라우드법은 미국 정부와 정식으로 상호 집행 협정을 맺은 외국 정부의 국민에 한해서만 기업이 법원에 이의를 제기할 수 있는 좁은 통로를 열어 두었습니다. 이천이십이년 이후 이런 협정을 맺은 나라는 영국과 오스트레일리아 두 곳뿐이며, 유럽연합은 아직 이런 협정을 미국과 맺지 않았습니다. 그러므로 유럽 시민의 정보에 관해서는 이 예외적 이의 제기 절차조차 적용되지 않습니다.

협정을 맺은 영국의 경우에도 이 통로는 넓지 않습니다. 요청 대상이 미국 국적자가 아니고 미국에 거주하지도 않아야 하며, 정보를 넘기는 행위가 영국 법과 실제로 충돌한다는 점을 회사가 입증해야만 법원이 이의를 받아들입니다. 유럽연합처럼 협정 자체가 없는 경우에는 이런 제한적인 통로마저 존재하지 않습니다. 셋째, 이 법이 미치는 범위는 회사의 국적과 지배 구조에 달려 있지, 서버의 물리적 위치에 달려 있지 않습니다. 미국과 아무런 지분 관계도 경영 관계도 없는 순수한 유럽 회사라면 클라우드법의 대상이 되지 않습니다.

이 구조를 하나의 구체적인 흐름으로 따라가 보면 이해가 쉽습니다. 프랑스의 어느 행정 부처가 미국 회사의 유럽 자회사와 계약을 맺으면서 데이터를 반드시 프랑스 영토 안에 두겠다는 조항을 넣었다고 가정하겠습니다. 이 계약은 프랑스 정부와 유럽 자회사 사이의 약속입니다. 그런데 미국 검찰이 그 데이터를 원한다면, 검찰은 프랑스에 있는 자회사가 아니라 미국에 있는 모회사에 영장을 보냅니다. 모회사는 자회사의 지분과 경영권을 쥔 주체이므로 법률상 그 데이터를 점유, 보관, 통제하는 지위에 있다고 간주됩니다.

모회사가 자회사에 데이터 제출을 지시하면, 자회사는 프랑스 정부와 맺은 계약과 무관하게 그 지시를 따를 수밖에 없습니다. 프랑스 정부는 계약의 상대방이었을 뿐 이 내부 지시 과정에는 개입할 권한이 없습니다. 데이터가 프랑스 영토를 한 번도 떠나지 않아도 이 절차는 그대로 진행됩니다. 데이터가 유럽에 머물러 있다는 조건만으로 법적 위험이

사라지지 않는 이유가 여기에 있습니다. 위험을 결정하는 것은 서버가 놓인 위치가 아니라 그 서버를 관리하는 회사의 국적과 지배 구조입니다.

여기에 또 하나의 층이 겹칩니다. 유럽연합의 개인정보보호규정 제사십팔조는 외국 법원이나 행정 당국이 개인정보 이전을 요구하더라도, 그 요구가 유럽연합이나 회원국과 맺은 국제 협정에 근거하지 않는 한 유럽 안에서 그대로 승인되거나 집행될 수 없다고 정합니다. 그런데 앞서 살펴본 대로 미국과 유럽연합 사이에는 클라우드법에 따른 상호 집행 협정이 없습니다. 결국 미국에서 영장을 받은 회사는 서로 다른 두 법 사이에 놓입니다.

미국 영장을 따르면 유럽연합법이 요구하는 국제 협정상의 근거 없이 정보를 넘기게 되고, 영장을 거부하면 미국 법정에서 법정모독 책임을 질 수 있습니다. 이 충돌은 서류상의 논쟁이 아니라 실제로 미국계 클라우드 기업들이 유럽 고객과 계약을 맺을 때마다 마주치는 구조적 딜레마입니다.

이탈리아의 사례는 이 딜레마가 얼마나 뿌리 깊은지 보여 줍니다. 이탈리아 정부는 공공 행정을 위한 자국 전략 클라우드인 폴로 스트라테지코 나치오날레를 세우면서 데이터를 이탈리아 영토 안에만 두고 암호화 열쇠도 자국 기관이 직접 관리하도록 설계했습니다. 그러나 이 전략 클라우드를 실제로 구동하는 하부 기술은 마이크로소프트 애저와 구글 클라우드 같은 미국계 하이퍼스케일러였습니다. 이탈리아 당국은 열쇠를 손에 쥐고 있어도 그 열쇠로 잠그는 자물쇠 장치 자체를 미국 회사가 설계하고 공급한다는 근본적인 한계를 완전히 지우지 못했습니다.

데이터 위치와 암호화 열쇠라는 두 겹의 방어막을 세워도 소프트웨어 원천 기술의 국적이라는 세 번째 층은 여전히 미국에 남아 있었습니다.

이 실체는 추상적 법 조문이 아니라 실제 증언으로 확인됐습니다. 마이크로소프트의 법무 담당 임원은 이천이십오년 칠월 십칠일 프랑스 상원 청문회에 출석해 선서한 뒤 증언했습니다. 그는 파리에 물리적으로 저장된 사용자 데이터라 하더라도, 미국 연방 수사기관이 클라우드법에 근거해 정보 제출을 요구하면 프랑스 정부의 승인 없이도 회사가 그 정보를 넘겨줄 수밖에 없다고 인정했습니다.

이천이십오년 칠월 이십이일 미국 경제지 포브스가 이 증언을 보도하면서, 유럽 전역의 조달 담당 공무원들은 자국 영토 안에 서버를 두는 정책만으로는 미국 법의 사정권을 벗어날 수 없다는 사실을 문서로 확인하게 됐습니다.

클라우드법과 짝을 이루는 또 다른 위협은 해외정보감시법 제702조입니다. 이 조항은 이천팔년에 제정된 해외정보감시법 개정안에 포함되어 있으며, 미국 국가안보국 같은 정보기관이 미국 영토 밖에 있는 외국인의 통신 기록과 인터넷 데이터를, 개별 대상자마다 법원의 영장 심사를 받지 않고도 수집할 수 있도록 허용합니다. 클라우드법이 수사기관의 개별 요구에 따른 법 집행 도구라면, 제702조는 정보기관이 해외 정보 수집이라는 명목으로 폭넓게 운용하는 감시 권한입니다. 이 조항은 시효가 정해진 한시법이어서 미국 의회가 몇 년마다 다시 손을 대야 합니다.

이천이십사년 사월 미국 의회는 정보 개혁 및 미국 안보법을 통해 제702조를 다시 연장하면서 이천이십육년 사월까지 효력을 두었습니다. 이후 의회는 시한을 유월 십이일까지 한 차례 더 늦췄고, 결국 새로운 연장 입법이 그 시점까지 통과되지 못해 법 조문 자체는 이천이십육년 유월 십이일 자정 효력을 잃었습니다. 다만 미국 해외정보감시법원이 이천이십육년 삼월에 이미 승인해 둔 일 년짜리 감시 인증은 법이 만료된 뒤에도 그대로 유지되도록 설계되어 있어, 실제 감시 권한은 이천이십칠년 삼월까지 계속 작동하는 상태입니다.

법 조문의 존폐와 실제 감시의 지속 여부가 이렇게 어긋나 있다는 사실 자체가, 이 권한을 법률 하나로 통제하기가 얼마나 어려운지 보여 줍니다. 이 감시망에는 평범한 시민만이 아니라 동맹국의 장성과 고위 외교관의 이메일 전송 경로도 포함되어 있다는 사실이 여러 보도를 통해 지적되어 왔습니다. 제702조가 실제로 어떻게 작동하는지는 이천십삼년 전직 미국 정보요원 에드워드 스노든의 폭로를 통해 구체적으로 드러났습니다.

당시 공개된 문건에 따르면 미국 국가안보국은 이 조항을 근거로 구글과 마이크로소프트, 야후 같은 미국 회사의 서버에서 외국인 이용자의 자료를 직접 넘겨받는 프리즘이라는 수집 체계를 운용하고 있었습니다. 이 폭로는 유럽 각국이 제702조를 서류상의 조문이 아니라 실제로 가동되는 감시 기반 시설로 받아들이게 된 계기였습니다.

이 감시 구조가 유럽 법정에서 처음으로 정면충돌한 사건이 슈렘스 판결입니다. 유럽연합사법재판소는 이천이십년 칠월 십육일 오스트리아 시민 막시밀리안 슈렘스가 제기한 소송에서, 미국의 감시 체계가 유럽 시민의 개인정보 자기결정권을 심각하게 침해한다고 판단하며 미국과 유럽연합 사이의 개인정보 이전 협정인 프라이버시 실드를 무효로 선언했습니다. 재판부가 문제 삼은 것은 다른 무엇도 아닌 제702조 같은 미국의 무영장 감시 권한이었습니다.

유럽 기업이 아무리 계약서에 개인정보 보호 조항을 촘촘히 넣어도, 그 정보가 미국 회사의 통신망을 거치는 한 미국 정보기관의 감시 권한 자체를 계약으로 막을 수는 없다는 것이 판결의 핵심이었습니다. 유럽연합 집행위원회도 이천이십육년 유월 삼일 발의한 클라우드·인공지능 개발법의 영향 평가서에서 클라우드법과 제702조 두 가지를 유럽 디지털 영토가 지닌 구조적 안보 결함으로 명확히 지목했습니다.

이 문제는 법 조문 해석에 그치지 않고 실제 조달 정책을 바꾸는 힘으로 작동했습니다. 독일 바덴뷔르템베르크주 내무부는 마이크로소프트 소프트웨어를 기반으로 한 공공 클라우드 사업인 델로스 클라우드의 실제 가동 조건을 정밀하게 분석했습니다. 분석 결과는 명확했습니다. 데이터센터 자체는 독일 연방정보기술보안청의 인증을 받아 독일 영토 안에서 운영되지만, 그 위에서 돌아가는 응용 소프트웨어의 설계와 통제 권한은 여전히 미국 마이크로소프트가 쥐고 있었습니다.

주 내무부는 응용 계층의 통제권이 미국 회사에 남아 있는 한, 미국 안보 당국이 소프트웨어 공급자에게 이용자 몰래 데이터 유출 경로를 심으라고 지시할 가능성 자체를 배제할 수 없다고 결론지었습니다. 데이터가 물리적으로 독일에 있다는 사실은 이 위험을 없애지 못했습니다.

비슷한 우려는 네덜란드에서 정부의 공식 결정으로 이어졌습니다. 미국계 종합 정보기술 기업 킨드릴은 이천이십오년 십일월 네덜란드의 솔비니티를 인수하겠다고 발표했습니다. 솔비니티는 네덜란드 시민 약 천육백오십만 명이 쓰는 전자 신분증 체계인 디지드의 기반 인프라를 운영하는 회사였습니다. 네덜란드 하원에서는 이 인수가 미국 사법 관할권을 통해 자국민의 민감한 신원 정보에 접근할 길을 열어 줄 수 있다는 우려가 이어졌고, 정부는 인수를 막는 절차에 들어갔습니다.

네덜란드 경제부 아르츠 국무차관은 이천이십육년 오월 이십육일 공공의 이익을 지켜야 한다는 이유로 킨드릴의 솔비니티 인수를 정식으로 차단한다고 발표했습니다. 정부가 밝힌 근거는 분명했습니다. 미국 법은 미국 회사가 소유한 해외 자회사의 서버에 저장된 정보라도 미국 당국이 확보할 수 있도록 이론적으로 허용하고 있다는 것이었습니다. 이천이십년에 설립된 네덜란드 투자심사국이 미국 기업의 인수를 막은 것은 이번이 처음이었습니다. 미국 싱크탱크 국제전략문제연구소는 이 결정을 유럽 여러 나라의 투자 심사 기준이 앞으로 어떻게 바뀔지 가늠하는 시금석이라고 평가했습니다.

영국에서는 물리적 위치와 무관하게 계약 자체가 국가 기밀을 미국 회사에 넘기는 형태로 문제가 드러났습니다. 미국의 데이터 분석 기업 팔란티어는 영국의 핵무기 연구 기관인 원자력무기시설과 천오백만 파운드 규모의 클라우드 지원 계약을 맺었습니다. 이천이십육년 일월 이 계약을 보도한 탐사매체 더너브에 따르면 이 계약은 정부의 공식 조달 공개 사이트에 등록되지 않았고, 국방부는 계약의 존재 자체를 확인도 부인도 하지 않았습니다.

같은 보도는 팔란티어가 영국 정부와 맺은 계약 전체를 합치면 육억칠천만 파운드에 이른다고 집계했는데, 핵무기 시설과의 계약은 그중 공개 명단에서 빠진 채로 알려진 규모였습니다. 영국 하원 과학기술위원회는 국가의 수사망과 보건 데이터를 미국 회사에 의존하는 현재 구조가 조달 체계의 심각한 취약점이라고 지적했습니다. 핵무기 관련 정보를 다루는 계약이 공개 조달 명단에서 빠져 있었다는 사실은, 물리적 국경 안에서 계약을 맺는다고 해서 정보 통제권까지 자국에 남는 것은 아니라는 점을 다시 확인시켜 주었습니다.

독일에서는 팔란티어와 관련된 또 다른 법적 충돌이 있었지만, 이 사건은 클라우드법이나 제702조가 아니라 독일 헌법의 문제였다는 점을 구분해야 합니다. 독일 연방헌법재판소는 이천이십삼년 이월 십육일 범죄 혐의가 없는 시민을 예측 분석하는 경찰 프로그램의 운용이 위헌이라고 판결했습니다. 위헌 판정을 받은 헤센데이터 시스템은 팔란티어의 고섬 플랫폼을 기반으로 만들어진 치안 프로그램이었습니다. 이 판결이 문제 삼은 것은 미국 법의 역외 적용이 아니라 독일 기본법이 보장하는 시민의 자기결정권이었습니다.

두 가지 문제는 발생 원인이 다르지만, 결과적으로 같은 결론을 가리켰습니다. 미국 회사의 소프트웨어에 국가 치안 정보를 맡기는 구조는 미국 법 때문이든 자국 헌법 때문이든 여러 방향에서 동시에 흔들릴 수 있다는 사실입니다.

미국의 역외 사법권이 정보 제출 요구의 범위를 넘어 제재의 도구로도 쓰일 수 있다는 사실이 확인됐습니다. 미국 재무부 해외자산통제국은 이천이십오년 팔월 이십일 이스라엘 총리 네타냐후에 대한 체포영장 발부에 관여한 국제형사재판소 판사들에게 제재를 부과했습니다. 프랑스 국적의 판사 니콜라 기유도 제재 대상에 포함됐습니다. 이후 그는 은행 카드 결제와 아마존 서비스 접근이 막혔다고 언론에 밝혔습니다. 같은 제재 대상에 오른 다른 국제형사재판소 관계자의 이메일 계정은 마이크로소프트에 의해 정지됐다는 보도가 나왔고, 마이크로소프트 측은 이를 부인했습니다.

이 사건은 클라우드법이나 제702조와는 다른 제재 법규에 근거하지만, 결이 같은 위험을 보여 줍니다. 미국 회사가 제공하는 결제와 통신, 클라우드 서비스에 의존하는 개인과 기관은 미국 행정부의 결정 하나로 일상적인 서비스 접근권을 한꺼번에 잃을 수 있습니다.

프랑스는 이 문제를 아예 인증 기준의 문장으로 못박았습니다. 프랑스 국립정보시스템보안청은 신뢰 클라우드 사업자에게 부여하는 세큐넘클라우드 인증 기준을 개정하면서, 데이터를 유럽 안에 두는 조건만으로는 부족하다고 명시했습니다. 이천이십오년에 개정된 세큐넘클라우드 삼점이 버전은 인증을 받으려는 사업자에게 본사 소재지와 데이터센터가 유럽연합 안에 있어야 한다는 요건에 더해, 회사의 자본과 의결권 구조가 클라우드법 같은 역외 효력을 지닌 제삼국 법률로부터 완전히 독립되어 있어야 한다는 요건을 새로 넣었습니다.

국제 사법 공조 절차를 거치지 않은 채 제삼국이 데이터 공개를 명령해도 그 명령이 통하지 않는 구조를 갖추어야 인증을 받을 수 있다는 뜻입니다. 프랑스 당국이 인증 기준 조문에 클라우드법을 사실상 지목해 넣었다는 사실은, 유럽의 정책 담당자들이 이 문제를 계약서의 신뢰 조항이 아니라 회사의 소유 구조로 풀어야 할 문제로 규정했음을 보여 줍니다.

이 여러 사례를 나란히 놓고 보면 하나의 결론이 드러납니다. 데이터를 유럽 영토 안에 두는 정책은 필요한 조치이지만 그것만으로 충분하지는 않습니다. 위험을 실제로 줄이려면 정보를 다루는 회사 자체가 미국의 소유와 지배, 소프트웨어 설계 권한에서 벗어나 있어야

합니다. 서버의 위치는 지도 위의 좌표일 뿐이고, 그 좌표 안의 정보를 실제로 여닫는 권한은 회사의 본사가 어느 나라 법 아래 있는지에 따라 결정되기 때문입니다. 유럽의 여러 정부가 물리적 데이터 주권에서 회사 지배 구조와 소프트웨어 원천 기술까지 심사 범위를 넓혀 가는 이유가 바로 여기에 있습니다.

유럽연합 집행위원회는 클라우드·인공지능 개발법의 영향 평가서에서 이 구분을 정책 언어로 옮겼습니다. 평가서는 데이터의 물리적 저장 위치, 암호화 열쇠의 관리 주체, 소프트웨어를 설계하고 지원하는 회사의 소유 구조를 서로 다른 세 개의 층으로 나누어 검토했습니다. 프랑스의 세큐넘클라우드 인증이 회사의 자본 구조에 손을 댄 것도, 이탈리아의 전략 클라우드가 암호화 열쇠까지 손에 쥐고도 완전한 독립을 선언하지 못한 것도, 이 세 개 층이 따로 움직이지 않고 함께 갖추어져야 실질적인 보호가 성립한다는 사실을 각자의 방식으로 증명한 사례들입니다.

■ 근거자료 1. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943 (Public Law 115-141), 2018년 3월 23일. 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), 2008년. 3. U.S.

Congress, Reforming Intelligence and Securing America Act (RISAA), 2024년 4월 20일. https://www.congress.gov/crs-product/R48592 4. Electronic Frontier Foundation, 'Victory! 702 has Expired!', EFF Deeplinks, 2026년 6월. 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, 2020년 7월 16일 판결. 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),

미국 연방대법원. 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, 2025년 7월 22일. 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, 2026년 6월 3일. 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, 2024년.

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, 2026년 5월 26일. 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, 2026년 6월. 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, 2026년 1월. https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley 16.

Bundesverfassungsgericht, 헤센데이터 예측 치안 프로그램 관련 판결, 2023년 2월 16일. 17. Irish Times, ''It's surreal': US sanctions lock International Criminal Court judge out of daily life', Irish Times, 2025년 12월 12일.

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, 2026년.

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, 2025년.

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, 2013년 6월 6일. 22. Center for Strategic and International Studies, 'The Kyndryl-Solvinity Case: A Barometer for Investment Security Reviews?', CSIS Analysis, 2026년.

https://www.csis.org/analysis/kyndryl-solvinity-case-barometer-investment-security-reviews

2.3. '에어갭(Air-Gap)'과 독자 아키텍처: 계약 조항을 넘어선 기술적 격리

마이크로소프트의 법무 책임자는 2025년 7월 프랑스 상원 청문회에서 선서를 마친 채 증언했습니다. 파리에 저장된 사용자 데이터라 해도 미국 연방 수사 기구가 클라우드 법에 근거해 정보 제출을 요구하면, 자사는 프랑스 정부의 승인 없이도 자료를 넘길 수밖에 없다고 밝혔습니다. 이 증언은 유럽의 행정 담당자들에게 하나의 사실을 분명히 알려주었습니다. 데이터를 자국 영토 안에 두는 조치와 계약서에 보안 조항을 채워 넣는 조치만으로는 미국 사법 관할권의 손이 닿는 범위를 벗어날 수 없다는 사실입니다.

계약서는 원래 거래 당사자들이 지키기로 합의한 약속을 문서로 남긴 것입니다. 유럽의 여러 정부도 미국 클라우드 기업과 계약을 맺으며 데이터를 역외로 옮기지 않겠다는 조항, 유럽 법원의 명령 없이는 정보를 넘기지 않겠다는 조항을 계약서에 넣어 왔습니다. 그러나 이런 조항은 계약 상대방인 기업이 자유롭게 그 약속을 지킬 수 있는 상황에서만 힘을 발휘합니다. 그 기업이 미국 법의 적용을 받는 한, 미국 정부가 자국법을 근거로 정보 제출을 명령하면 기업은 계약서의 약속과 자국 법 사이에서 선택해야 하고, 대부분의 경우 자국 법을 따를 수밖에 없습니다.

상대 기업이 자국 정부의 명령과 계약상의 약속 가운데 하나를 고르도록 강요받는 순간, 계약서의 문구는 더는 보호막이 되지 못합니다.

이 사실은 유럽 여러 나라가 오랫동안 의지해 온 안전장치 하나를 무너뜨렸습니다. 유럽연합의 개인정보 보호 규정은 오래전부터 데이터를 역내에 저장하도록 요구해 왔고, 많은 공공 기관은 서버가 자국 국경 안에 있으면 정보가 안전하다고 여겨 왔습니다. 이런 요구를 데이터 지역화라고 부릅니다. 그러나 데이터 지역화는 정보가 물리적으로 어느 나라에 놓여 있는지를 규정할 뿐, 그 정보를 처리하는 소프트웨어를 누가 설계하고 누가 원격으로 접속할 권한을 쥐고 있는지는 규정하지 않습니다. 서버의 위치와 시스템의 통제권은 서로 다른 문제입니다.

독일 바덴-뷔르템베르크주 내무부의 분석은 이 차이를 구체적으로 드러냈습니다. 주 정부가 검토한 델로스 클라우드 사업은 데이터를 독일 영토 안의 서버에 물리적으로 보관하는 방식으로 설계되어 있었습니다. 그러나 이 클라우드를 실제로 움직이는 응용 프로그램의

설계와 갱신 권한은 여전히 미국 마이크로소프트 본사가 쥐고 있었습니다. 주 내무부는 이 사실을 근거로, 데이터가 독일 땅에 놓여 있어도 시스템의 통제권이 미국 기업 손에 남아 있는 한 클라우드 법의 수색 사정권에서 한 발짝도 벗어나지 못한다고 결론지었습니다.

데이터가 어디에 저장되어 있는지가 문제가 아니라, 그 데이터를 다루는 소프트웨어를 누가 설계하고 누가 갱신 명령을 내리는지가 문제였습니다.

프랑스가 국내보안총국의 정보 시스템으로 택한 아르곤OS는 이 두 사례가 드러낸 문제에 다른 방식으로 응답합니다. 아르곤OS를 개발한 햅스비전은 자본 지분 전체를 유럽 주주들이 소유한 기업입니다. 이 시스템은 외부 유선망과 완전히 끊어진 에어갭 환경이나, 외부 접속이 차단된 주권 클라우드 서버 위에서만 가동됩니다. 시스템을 소유한 회사에 미국 법인이 없고, 시스템이 놓인 네트워크에 외부로 뻗어 나가는 통로가 없다면, 미국 사법 기구가 영장을 발부해도 그 영장을 집행할 통로 자체가 존재하지 않습니다.

계약서에 적힌 약속이 아니라 네트워크 구성과 소유 구조가 격리를 만들어 내는 방식입니다.

이 격리에는 데이터 자체를 지키는 조치를 넘어서는 부분이 하나 더 있습니다. 아르곤OS는 수만 건에 이르는 이기종 정형, 비정형 데이터를 처리하면서 그 데이터를 잠그는 암호화 열쇠의 생애 주기를 자체적으로 관리하도록 설계되었습니다. 데이터가 암호화되어 있어도 그 열쇠를 외부 기업이 관리한다면, 열쇠를 쥔 쪽은 언제든 자물쇠를 열 수 있습니다. 암호화 열쇠 관리를 외부 접근으로부터 완전히 분리해 둔다는 것은, 데이터의 내용뿐 아니라 그 데이터를 읽을 수 있는 권한 자체를 자국 안에 가두어 둔다는 뜻입니다.

서버 위치와 암호 해제 권한을 함께 확보해야만 격리가 실제로 작동합니다.

에어갭이라는 말은 문자 그대로 컴퓨터 네트워크와 외부 인터넷 사이에 물리적인 공백을 두는 방식을 가리킵니다. 케이블이 연결되어 있지 않으므로, 원격에서 접속 차단 명령을 내리거나 시스템을 강제로 정지시킬 방법이 없습니다. 2026년 6월에 벌어진 페이블 5 접속 차단 사건은 정확히 이 지점을 겨냥한 사례였습니다. 앤트로픽의 모델은 인터넷을 통해 서비스되었고, 미국 상무부의 명령 한 장으로 해외 접속이 몇 시간 만에 전면 정지되었습니다. 외부 네트워크에 의존하는 서비스라면 계약이 아무리 두터워도 공급자의

본사가 위치한 국가의 행정 명령 앞에서 무력합니다.

반대로 외부와 연결된 통로 자체가 없는 시스템이라면, 그런 명령을 전달할 물리적 경로가 없습니다.

다만 에어갭 아키텍처를 갖춘다고 해서 곧바로 안전이 완성되지는 않습니다. 프랑스 내무부는 국내보안총국이 아르곤OS로 실전 정보 활동 전체를 이식하는 데 18개월에서 24개월이 걸릴 것이라고 밝혔습니다. 수십 년간 팔란티어의 화면 조작 방식에 익숙해진 요원들은 새 시스템에 다시 적응해야 하고, 기존에 쌓인 데이터의 저장 표준 자체가 미국 시스템에 맞추어 설계되어 있어 이식 과정에서 정보가 누락되거나 형식이 어긋날 위험이 남습니다. 프랑스 국가 행정부는 이 공백을 메우기 위해 2027년까지 옛 체계와 새 체계를 함께 운용하는 과도기를 두겠다고 약속했습니다.

격리된 아키텍처로 옮겨 가는 결정과 그 아키텍처가 실제로 완전하게 가동되는 시점 사이에는 몇 년의 간격이 놓여 있고, 그 몇 년 동안 두 개의 서로 다른 체계를 동시에 유지하는 부담은 고스란히 정보기관의 몫으로 남습니다.

이 간격 동안 치르는 비용은 이식 기간에 그치지 않습니다. 외부 네트워크와 끊어진 시스템은 대형 클라우드 기업이 제공하는 실시간 업데이트와 위협 정보 공유 서비스로부터도 함께 끊어집니다. 아르곤OS 같은 독자 시스템을 운용하는 기관은 보안 패치와 기능 개선을 자체 인력으로 감당해야 하며, 이는 미국 대형 클라우드 기업의 전 세계 데이터센터 네트워크가 자동으로 제공하던 규모의 경제를 포기하는 선택이기도 합니다.

외부와 연결된 통로 자체가 없는 환경에서는 소프트웨어 갱신조차 인터넷을 통한 자동 배포로 처리할 수 없고, 검증을 마친 저장 장치에 담아 물리적으로 반입하는 절차를 거쳐야 하는 경우가 많습니다. 이런 절차는 인터넷 갱신보다 느리고, 갱신 내용을 매번 확인하는 별도의 검증 인력을 요구합니다. 유럽의 정책 결정자들이 격리를 선택하면서도 이를 만능 해법으로 내세우지 않는 이유가 여기에 있습니다. 격리는 외국 정부의 일방적 명령이 시스템을 정지시키는 위협을 막아 주지만, 그 대가로 상시적인 유지 보수의 부담을 자국이 떠안아야 합니다.

에어갭이 해결하는 문제와 해결하지 못하는 문제를 가르는 기준은 그 시스템이 얼마나 많은 연산 자원을 필요로 하는가에도 있습니다. 아르곤OS처럼 한 기관의 정보 분석을 담당하는 시스템은 상대적으로 제한된 규모의 서버로도 완전히 격리된 환경에서 가동할 수 있습니다. 그러나 페이블 5처럼 방대한 연산을 상시로 요구하는 대형 인공지능 모델은 사정이 다릅니다. 이런 모델을 자국 영토 안에서 외부와 끊어진 채로 학습시키고 운용하려면 개별 기관 하나가 감당할 수 없는 규모의 데이터센터와 전력, 반도체가 필요합니다.

페이블 5 차단 사건이 유럽에 남긴 과제가 개별 시스템의 에어갭을 넘어 대륙 규모의 연산 인프라를 갖추는 문제로 번진 이유가 여기에 있습니다.

스위스와 네덜란드의 대응은 격리에 이르는 경로가 하나가 아님을 보여줍니다. 스위스 연방 기관들은 2018년부터 2025년까지 팔란티어의 입찰 제안을 최소 아홉 차례 거절하며 애초에 이 기업의 시스템을 들이지 않았습니다. 이미 도입한 시스템을 걷어 내고 새 아키텍처로 옮기는 프랑스나 독일과 달리, 스위스는 이식이라는 값비싼 과정 자체를 겪지 않았습니다. 네덜란드 국방부는 2026년 6월에 이개년 안에 팔란티어를 대체하겠다는 로드맵을 의회에 제출했지만, 로드맵은 아직 계획이며 실제로 옛 시스템이 꺼지고 새 시스템이 전면 가동되는 시점은 그 이후입니다.

처음부터 의존을 만들지 않는 선택과, 이미 생긴 의존을 걷어 내는 선택은 같은 목적지를 향해도 치르는 비용이 다릅니다.

격리를 완성한 상태도 영구히 고정되지는 않습니다. 네덜란드 행정망의 핵심 소프트웨어를 공급하던 현지 기업 솔비니티를 미국계 기업 킨드릴이 인수하겠다고 발표하자, 네덜란드 하원은 자국 시민 1650만 명의 정보를 다루던 인프라의 소유권이 하루아침에 미국 기업으로 넘어갈 수 있다는 사실에 큰 우려를 표했습니다. 오늘 유럽 기업이 소유한 시스템이라 해도, 그 기업이 내일 외국 자본에 인수되면 소유 구조를 조건으로 삼았던 격리는 그대로 무너집니다.

격리를 증명하는 절차가 도입 시점의 일회성 심사에 그쳐서는 안 되고, 소유권과 지배 구조의 변동을 지속적으로 확인하는 절차로 이어져야 하는 이유가 여기에 있습니다.

격리 아키텍처가 만들어 내는 마찰은 국경을 넘는 군사 협력에서도 드러납니다. 북대서양조약기구 보안인증위원회가 2026년 6월 22일 팔란티어의 메이븐 스마트 시스템을 완전 무기 작전용으로 공인한 상황에서, NATO 최고 사령관들은 개별 회원국이 치안과 행정 영역에서 벌이는 탈팔란티어 조치를 군사 전장 효율성을 깎아내리는 결정이라고 비판했습니다. 국내 치안 정보망을 외부와 끊어진 아르곤OS로 옮기는 선택과, 동맹군이 공유하는 표적 정보망이 여전히 팔란티어의 소프트웨어 위에서 돌아가는 현실은 같은 나라 안에서 부딪칩니다.

한 국가의 정보기관이 자국 영역에서 격리를 완성해도, 그 나라가 속한 동맹 전체의 정보망까지 격리할 수는 없습니다. 격리의 경계를 어디까지 그을 것인지는 기술의 문제인 동시에 동맹 관계를 어떻게 유지할 것인지를 정하는 정치적 선택이기도 합니다.

정치적 선언과 아키텍처의 완성 사이에도 틈이 남습니다. 르코르뉘 장관이 아르곤OS 전환을 발표한 뒤에도 팔란티어 사는 자사가 국내보안총국과 맺은 기존 계약이 여전히 법적으로 유효하다고 밝혔습니다. 정부의 발표와 조달 절차의 전환, 계약의 실제 종료, 시스템의 완전한 교체는 같은 날 한꺼번에 일어나는 사건이 아닙니다. 정치적 선언이 나온 시점과 옛 시스템이 실제로 꺼지는 시점 사이에는 협상과 이행이라는 별도의 과정이 남아 있고, 그 기간 동안 옛 계약은 문서상으로 여전히 살아 있을 수 있습니다.

계약을 끊겠다는 발표 자체는 격리를 완성하지 않으며, 완성의 증거는 발표문이 아니라 실제로 작동을 멈춘 옛 시스템과 실제로 가동을 시작한 새 시스템에 있습니다.

프랑스와 독일의 이런 결정은 유럽연합 차원의 법이 만들어지기를 기다리지 않고 각국 정부가 먼저 내린 결정이었다는 점에서도 눈여겨볼 만합니다. 국내보안총국의 아르곤OS 전환과 연방헌법수호청의 같은 선택은 모두 개별 국가의 조달 절차를 통해 이루어졌습니다. 이는 계약과 조달이라는 익숙한 절차 안에서도 공급 기업의 소유 구조와 네트워크 구성을 조건으로 요구하면 실질적인 격리를 만들어 낼 수 있음을 보여줍니다. 법이 뒤따라오기 전에 개별 국가가 먼저 아키텍처 자체를 바꾸어 놓았고, 유럽연합의 다음 과제는 이런 개별 사례를 공통의 조달 기준으로 옮기는 일이었습니다.

유럽연합 집행위원회는 이 격리의 원칙을 개별 기업의 선택에 맡기지 않고 조달 규정으로 옮기려 하고 있습니다. 집행위원회가 2026년 6월 내놓은 클라우드·AI 개발법 제안은 아직

유럽의회와 이사회의 심의를 거쳐야 하는 법안 초안이며, 제정된 법률이 아닙니다. 그럼에도 이 제안은 공급 기업의 소유 구조와 이사회 국적, 소스코드에 대한 외부 접근 여부까지 심사하는 등급 체계를 마련해, 계약서의 약속이 아니라 시스템 자체의 설계로 격리를 증명하도록 요구하는 방향을 잡고 있습니다.

가장 높은 등급에서는 시스템의 설계와 소스코드의 유지 보수 전 과정에서 외국 자본의 간섭을 조금도 허용하지 않는 수준의 격리를 요구하는 안이 논의되고 있습니다.

이런 심사 체계가 뜻을 지니려면 격리를 증명하는 절차 자체가 공급 기업의 자기 신고에 그쳐서는 안 됩니다. 프랑스가 이미 운용해 온 독자 인증 규범인 섹넘클라우드는 정부가 지정한 심사 기관이 소프트웨어 설계 도면과 소스코드를 정기적으로 감사하는 방식을 취하고 있습니다. 에어갭이나 주권 클라우드라는 이름표를 붙였다는 이유만으로 격리가 완성되었다고 볼 수는 없습니다. 네트워크 구성도와 소유 지분 등기부, 소스코드 저장소를 외부 감사자가 직접 확인할 수 있을 때에야 그 이름표는 실체를 갖습니다.

클라우드·AI 개발법 제안에는 유럽연합 사이버보안청이 운영하는 인증 체계에서 최고 등급의 자격을 요구하는 방안도 담겨 있어, 국가 차원의 인증과 연합 차원의 인증이 함께 격리를 확인하는 이중 구조로 설계되고 있습니다.

계약과 아키텍처는 서로를 대체하는 관계가 아니라 함께 작동해야 하는 관계입니다. 계약은 조달 가격과 서비스 품질, 책임 소재를 정하는 문서로서 지금도 필요합니다. 다만 국가 안보처럼 외국 정부의 개입 가능성 자체를 차단해야 하는 영역에서는, 계약이 약속하는 보호를 시스템의 물리적 구성과 소유 구조가 뒷받침하지 못하면 그 약속은 위기의 순간에 지켜지지 않습니다.

계약 조항은 상대가 약속을 지킬 의지가 있을 때에만 작동합니다. 미국의 클라우드 법과 해외정보감시법 제702조는 미국 기업에 대해 국가가 그 의지를 거두어들일 권한을 이미 쥐고 있음을 보여주었고, 페이블 5 접속 차단 사건은 그 권한이 동맹국을 상대로도 실제로 행사될 수 있음을 증명했습니다. 유럽의 정보기관과 행정 부처들이 에어갭과 소유 구조 격리로 방향을 튼 이유는 계약서가 약속하는 보호와 네트워크 설계가 실제로 만들어 내는 보호 사이에 간격이 있다는 사실을 겪어 냈기 때문입니다.

그 간격을 메우는 작업은 법 조항 하나로 끝나지 않고, 몇 년에 걸친 이식과 자체 유지 보수, 그리고 독립된 감사라는 세 가지 조건이 함께 갖추어질 때에만 완성됩니다.

■ 근거자료 1. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026년 6월 17일, 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, 2025년 7월 22일, https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/ 3. 저자 미상, '유럽의 팔란티어 이탈 흐름을 원 소스까지 확인해 정리했습니다', 2026년. 4.

ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, 2026년 6월 16일. 5. Loïc Duval, 'La DGSI remplace Palantir par ChapsVision', InformatiqueNews, 2026년 6월 18일. 6.

저자 미상, 'La DGSI prépare la sortie progressive de Palantir au profit de ChapsVision', Solutions Numériques, 2026년 6월 17일. 7. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026년, 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), 2026년 7월 7일. 9. 출처 없음(일반 지식 보충). (→ 데이터 지역화와 기술적 격리의 개념적 차이, 에어갭 시스템이 외부 클라우드의 실시간 갱신과 규모의 경제로부터 단절되어 자체 유지 보수 부담을 진다는 일반적 기술 원리를 보완합니다.)

제3장. 디지털 주권의 이중 구조: 국가 자립과 NATO 동맹의 균열

3.1 국내 정보 영역과 군사 동맹 영역의 차이

2026년 6월 16일, 프랑스의 세바스티앙 르코르뉘 총리는 국내보안총국(DGSI)이 써 온 미국 팔란티어의 프로그램을 프랑스 기업 햅스비전(ChapsVision)이 만든 아르곤OS로 옮기겠다고 발표했습니다. 같은 날 르몽드는 팔란티어 쪽이 정부와 맺은 계약이 여전히 유효하다고 주장한다고 함께 보도했습니다. 발표와 계약 종료, 실제 시스템 교체는 서로 다른 시점에 이루어지는 별개의 절차입니다. 6월 16일의 뉴스는 전환을 시작하겠다는 선언이지, 아르곤OS로의 이식이 끝났다는 확인은 아닙니다.

독일 연방헌법수호청(BfV)도 비슷한 길을 걸었습니다. 2026년 5월, BfV는 미국 감시 소프트웨어 대신 햅스비전의 아르곤OS를 새로 들이기로 결정했다고 여러 독일 매체가 전했습니다. 네덜란드 국방부는 2026년 6월, 앞으로 2년 안에 팔란티어 소프트웨어를 완전히 걷어내겠다는 계획을 내놓았습니다. 스위스 연방 기구들은 2018년부터 2025년 사이에 팔란티어가 낸 정보 입찰을 최소 아홉 차례 거절했다고 알려졌습니다. 스위스의 이 거절은 어느 한 정부가 급하게 내린 결정이 아니라, 여러 해에 걸쳐 반복된 조달 판단이었습니다.

스페인에서도 같은 흐름이 나타났습니다. 페르난도 그란데마를라스카 내무장관은 국가헌병대(과르디아 시빌)와 팔란티어가 함께 진행하던 데이터 분석 사업을 중단시켰습니다. 스페인 군사정보센터가 2023년에 맺은 1650만 유로 규모의 계약은 만료된 뒤 연장되지 않았습니다. 군 수뇌부는 계약 유지를 요청했지만 받아들여지지 않았습니다. 스페인 정부는 그 대신 자국 기술전환공사를 통해 7억 2000만 유로를 들여 독자적인 인공지능 데이터센터를 짓기로 했습니다. 벨기에 정부는 2029년까지 10억 유로를 투입해 군용 데이터 저장 시설을 자체적으로 세우겠다고 밝혔습니다.

영국에서는 갈등이 더 크게 드러났습니다. 영국 하원 과학혁신기술위원회는 공공 데이터 분석망을 미국의 민간 기업에 넘긴 구조를 안보상의 취약점이라고 지적하는 보고서를 냈습니다. 영국 국가보건서비스(NHS)와 팔란티어가 맺은 3억 3000만 파운드 규모의 계약을 두고 하원의원들은 계약을 끝내야 한다고 요구했습니다. 이들은 그만한 비용을 치르고도 데이터 구조를 설계하는 온톨로지 권한을 넘겨받지 못했다는 점을 문제로 짚었습니다. 계약이 끝나도 영국 정부의 손에 남는 기술 자산이 없다는 뜻입니다.

하원은 2027년 2월부터 발동하는 주권 사유 해지권 조항을 근거로 팔란티어와의 관계를 정리하라고 정부에 권고했습니다. 덴마크 의회에서도 2025년 5월, 야당이 미국 소프트웨어 의존을 끊자는 안건을 냈습니다.

이 결정들은 모두 한 나라 안에서 내려졌습니다. 국내 정보기관과 국방부는 자국의 경찰 기록과 첩보 자료를 스스로 관리할 권한을 갖고 있습니다. 계약을 끝내고 다른 회사의 제품으로 옮기는 절차도 그 권한 안에서 비교적 빠르게 진행할 수 있습니다. 여기에는 법률적인 이유가 있습니다. 미국 의회가 2018년 3월에 제정한 클라우드법은 미국 법인이 경영을 통제하는 서비스라면, 자료가 저장된 서버가 어느 나라에 있든 미국 수사기관의 정식 요청에 자료를 내놓아야 한다고 정합니다.

이 조항이 실제로 어떤 사건에 적용되었는지, 그 요청이 매번 합법적으로 처리되었는지는 사건마다 다르게 판단해야 할 문제입니다. 다만 이 법이 존재한다는 사실만으로도 유럽의 정보기관들은 자국의 수사 자료가 미국 기업의 서버 구조 안에 있는 상태를 부담으로 받아들였습니다.

같은 시기 다자간 군사동맹의 결정은 반대 방향으로 움직였습니다. 북대서양조약기구(NATO) 산하 통신정보국(NCIA)은 2025년, 팔란티어의 메이븐 스마트 시스템을 연합작전사령부에서 쓰기 위한 계약을 맺었습니다. 이 계약은 요구 사항을 정하는 단계부터 서명까지 약 6개월 만에 끝났습니다. 나토 보안인증위원회는 그로부터 1년 넘게 지난 2026년 6월, 이 시스템의 완전한 기술적 작전 능력을 확인했습니다. 조달 계약을 맺은 시점과 완전 운용 능력을 인증받은 시점은 같은 사건이 아니며, 그 사이에는 검증과 시험을 거치는 긴 기간이 있었습니다.

이 차이가 생기는 이유는 두 영역이 다루는 업무의 구조 자체가 다르기 때문입니다. 국내 정보기관 하나가 쓰는 시스템은 그 나라 국경 안에서, 그 나라 법을 따르는 요원들만 접속합니다. 프랑스 국내보안총국의 수사관이 작성한 사건 기록은 아르곤OS 안에서 프랑스어로 저장되고, 프랑스 검찰과 법원의 절차를 거쳐야만 밖으로 나갑니다. 반면 메이븐 스마트 시스템은 처음부터 서른 개가 넘는 나라의 군인이 같은 화면을 보고 같은 표적 목록을 공유하도록 설계되었습니다.

미군의 아넬 데이비드 대령은 이 시스템 안에서 개발한 전술 응용 프로그램이 50개가 넘는다고 밝혔고, 이 프로그램들은 나토 연합군의 통신 표준인 스탠악(STANAG) 4774와 4778을 따르도록 만들어졌습니다. 표준을 따른다는 것은 폴란드 군인이 입력한 좌표를 노르웨이 군인이 곧바로 읽고, 미군 조종사가 그 좌표로 항로를 잡을 수 있다는 뜻입니다. 국내 수사 기록은 국경을 넘지 않아야 안전하고, 연합 작전의 표적 정보는 국경을 넘어야 쓸모가 있습니다. 두 업무는 안전의 기준 자체가 반대 방향을 가리킵니다.

나토 최고위 인사들은 이 차이를 정치적 선택이 아니라 군사적 필요로 설명합니다. 나토의 최고 변혁사령관 피에르 방디에 프랑스 해군 대장은 유럽 군대가 위성 영상을 자동으로 분석하고 탄약 보급을 조율하는 데 쓸 만한 자체 소프트웨어를 아직 갖고 있지 않다고 인정했습니다. 그는 대체할 기술이 무르익기 전에 동맹의 작전 수행 능력을 떨어뜨릴 수는 없다고 말했습니다. 카이 로어슈나이더 사령관을 비롯한 다른 지휘관들도 회원국이 각자 다른 시스템을 쓰면 암호화된 통신망 사이의 연결이 끊어질 수 있다고 경고했습니다.

이들의 논리는 국가 하나가 정보 주권을 지키려다 동맹 전체의 통신 체계를 약하게 만든다면, 그 손해가 더 크다는 것입니다.

이 논리에는 반박도 따릅니다. 회원국들이 자국 안보 영역에서 팔란티어를 배제한 이유는 미국의 국내법이 미국 기업의 서버에 접근할 권한을 미국 수사기관에 준다는 데 있습니다. 이 우려를 국내 정보망에서는 심각하게 받아들이면서 나토 지휘 체계 안에서는 받아들이지 않는다면, 그 기준은 데이터의 성격이 아니라 계약 상대가 국내 기관인지 다국적 동맹인지에 따라 갈라집니다.

이 모순은 자본의 흐름에서도 드러납니다. 독일 인터넷 매체 넷츠폴리틱(netzpolitik.org)의 보도에 따르면, 유럽 여러 나라의 은행과 자산운용사들은 자국 정부가 팔란티어와 거리를 두는 동안에도 팔란티어 주식을 사들이는 규모를 오히려 늘렸습니다. 팔란티어는 2026년 2분기 실적 발표에서 매출이 1년 전보다 93퍼센트 늘었다고 밝혔습니다. 공공 부문은 팔란티어에서 걸어 나갔고, 민간 자본은 같은 시기에 팔란티어로 더 가까이 다가갔습니다.

이보다 앞서 독일 연방헌법재판소는 2023년 2월 16일, 헤센주 경찰이 팔란티어의 고섬 엔진을 바탕으로 만든 자동 데이터 분석 시스템 헤센데이터에 위헌 결정을 내렸습니다.

재판소는 개인의 자료를 자동으로 결합해 위험 인물을 가려내는 이 시스템에 충분한 법적 근거가 없다고 판단했습니다. 이 판결은 유럽연합 인공지능법이 만들어지기도 전에 나온 것으로, 국내 헌법 질서가 국가안보 예외와 별개로 국내 치안용 인공지능 시스템을 통제할 수 있다는 사실을 먼저 보여준 사례입니다.

국가 하나의 헌법재판소는 자국의 경찰 시스템에 제동을 걸 힘을 갖고 있습니다. 그러나 서른두 개 나라가 함께 쓰는 동맹 지휘 체계에는 그런 제동 장치를 가진 단일 기관이 없습니다. 국내 정보 영역의 이탈과 군사 동맹 영역의 확대는 통제할 수 있는 주체가 있는 영역과 없는 영역의 차이에서 갈라집니다.

근거자료

1. 프랑스 상원 조사위원회, '유럽연합(EU) 주요국의 탈(脫)팔란티어 행보와 디지털 주권화에 관한 분석 보고서', 프랑스 정부 공식 포털, 2026.

2. 존 헨리, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026년 6월 16일.

3. 기자 미상, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026년 6월 17일.

4. 저자 미상, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, 2026년 5월 26일.

5. IT-Daily 편집국, 'Palantir: Bundesamt für Verfassungsschutz wählt ChapsVision', IT-Daily, 2026년 5월.

6. 콜린 바크, 'Defensie wil binnen twee jaar af van Palantir-software', ICTMagazine, 2026년 6월 3일.

7. Egl⌧ Kri⌧topaityt⌧, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, 2026년 7월 2일.

8. Le Soir 편집국, 'Palantir s'implante en Belgique: 28 questions à (se) poser', Le Soir, 2026년 3월 19일.

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

10. 영국 하원 과학기술위원회, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', UK Parliament, 2026.

11. 얀 에벌, '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. 독일 연방헌법재판소, 'Decisions search - Judgment of 16 February 2023', 독일 연방헌법재판소, 2023년 2월 16일.

14. 저자 미상, '유럽의 팔란티어 이탈 흐름을 원 소스까지 확인해 정리한 자료', 2026. (스위스 아홉 차례 입찰 거절 및 덴마크 야당 제안 근거)

15. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE 공식 보도자료, 2026년 6월 30일.

16. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.
17. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018.

3.2 NATO '메이븐 스마트 시스템(MSS)'의 완전 운용 능력 획득과 상호 운용성의 덫

미국 국방부는 2017년, 인공지능으로 드론과 위성 영상을 분석해 군사 표적을 찾아내는 프로젝트 메이븐을 시작했습니다. 팔란티어는 이 계획을 발판으로 상업용 버전을 만들었고, 이 상업용 버전이 나토가 도입한 메이븐 스마트 시스템의 뿌리입니다.

나토 통신정보국(NCIA)은 2025년, 이 시스템을 연합작전사령부에서 쓰기 위한 계약을 팔란티어와 맺었습니다. 조달 요구 사항을 정하는 단계부터 계약서에 서명하는 순간까지 걸린 기간은 약 6개월이었습니다. 이 시점에서 나토가 확보한 것은 시스템을 쓸 수 있는 권리와 계약이었지, 모든 군사 활동에서 아무 때나 쓸 수 있다는 인증은 아니었습니다.

완전한 기술적 작전 능력, 곧 FOC(Full Operational Capability) 인증은 그로부터 1년 넘게 지난 뒤에 나왔습니다. 나토 보안인증위원회는 2026년 6월 22일, 메이븐 스마트 시스템이 기밀망에서 운용할 수 있는 수준에 이르렀다고 확인했습니다. NCIA의 바르트 판 미어트 최고운영책임자 대행은 6월 26일, 이 인증 결과를 동맹국 사령부에 보고했습니다. 나토 최고사령부(SHAPE)는 6월 30일, 이 시스템이 훈련과 실전을 포함한 모든 군사 활동 영역에서 제한 없이 쓰일 수 있다고 공식 발표했습니다.

NCIA의 딜런 브라운 총지배인은 연합군 전투원들에게 이 능력을 넘겨준 협력을 자랑스럽게 여긴다고 밝혔습니다.

계약을 맺은 2025년과 완전 운용을 인증한 2026년 사이에는 검증의 기간이 있었습니다. 이 시스템은 2026년 5월 13일 노르웨이에서 끝난 다국적 훈련 스테드패스트 디터런스에서 실전과 비슷한 상황을 거쳤습니다. 독일 연방군의 루프레히트 폰 부틀러 소장은 이 훈련에서 인공지능이 가상 적군의 행동 시나리오를 자동으로 만들어내는 성능을 확인했다고 말했습니다.

메이븐 스마트 시스템은 군사 위성과 드론, 레이더가 보내는 자료를 실시간으로 모아 분석합니다. 군인들은 이 화면을 보고 타격 표적을 골라내는 시간을 크게 줄일 수 있습니다. 미군의 아넬 데이비드 대령은 이 시스템 안에서 개발한 전술 응용 프로그램이 50개가 넘는다고 밝혔고, 이 프로그램들은 연합군의 통신 표준인 스탠악 4774와 4778을 따르도록

만들어졌습니다. 이 표준을 지킨다는 것은 회원국 군대가 서로 다른 나라의 군대와 표적 정보를 안전하게 주고받을 수 있다는 뜻입니다.

팔란티어 쪽은 데이터 소유권 문제에 분명한 입장을 냈습니다. 팔란티어에서 파견된 피오나 브래들리는 메이븐 스마트 시스템 안의 모든 소프트웨어와 데이터 소유권이 나토 동맹에 있다고 말했고, 자사는 고객의 자료를 마음대로 가공해 되파는 회사가 아니라고 밝혔습니다. 이 설명은 데이터가 누구의 것이냐는 질문에는 답을 주지만, 그 데이터를 다루는 프로그램의 구조를 누가 설계하느냐는 다른 질문에는 답이 되지 않습니다.

시스템의 핵심 코드와 데이터 분류 체계, 곧 온톨로지를 고치는 권한은 여전히 팔란티어의 민간 기술진에게 있습니다. 나토 회원국 군인이 입력한 표적 좌표는 계약상으로는 동맹의 자산이지만, 그 좌표를 정리하고 분류하는 방식은 팔란티어가 정한 틀 안에서만 움직입니다. 도서관에 비유하면, 책의 소유권은 도서관에 있어도 책을 어떤 순서로 분류해 꽂을지 정하는 사서 자리에는 여전히 팔란티어 직원이 앉아 있는 구조에 가깝습니다. 데이터 소유권과 시스템 설계권은 같은 종류의 주권이 아니며, 나토가 확보한 것은 앞쪽이고 뒤쪽은 여전히 팔란티어 안에 남아 있습니다.

이 시스템의 성능은 실제 작전에서 시험대에 올랐습니다. 미군은 2026년 2월, 이란과 연계된 무장 단체를 겨냥한 공습을 준비했습니다. 군은 공습을 시작한 뒤 첫 24시간 동안 메이븐 스마트 시스템을 돌려 1000개가 넘는 타격 후보 지점을 추려냈습니다. 이 결과를 지켜본 연합군 지휘관들은 미국 소프트웨어의 처리 속도에 신뢰를 나타냈습니다.

같은 시기 프랑스와 독일, 네덜란드는 정반대의 결정을 국내 영역에서 내리고 있었습니다. 프랑스는 6월 16일 국내보안총국의 소프트웨어를 아르곤OS로 옮기겠다고 선언했고, 독일 연방헌법수호청도 5월에 같은 결정을 내렸습니다. 독일 연방군의 토마스 다움 부제독은 4월, 국방 클라우드 사업의 최종 조달 규격에서 팔란티어를 뺐습니다. 나토 지휘부 상단이 팔란티어의 시스템으로 더 깊이 들어가는 동안, 같은 나라들의 국내 정보와 국방 조달망은 같은 회사에서 더 멀리 걸어 나가고 있었습니다.

이 두 방향의 움직임은 나토 안에서 마찰을 일으켰습니다. 방디에 사령관은 유럽 군대가 위성 영상 분석이나 탄약 보급 조율에서 팔란티어에 맞먹는 자체 소프트웨어를 아직 갖고 있지 않다고 인정했습니다. 그는 대체 기술이 무르익기 전에 동맹의 작전 능력을 깎아낼

수는 없다고 말했습니다. 독일의 카이 로어슈나이더 사령관은 회원국이 각자 자기 나라에서 만든 시스템을 따로 쓰면 암호화 통신망 사이의 연결이 끊어질 위험이 있다고 경고했습니다.

이에 맞서 프랑스는 자체 대안을 실험하기 시작했습니다. 프랑스 국방부는 2026년 6월, 폴란드에서 열린 조달 훈련에서 아르카디아 플랫폼을 시험했습니다. 아르카디아는 프랑스의 방산기업 탈레스와 사프란, 그리고 미스트랄 AI가 함께 만든 전장 인지 소프트웨어입니다. 프랑스 육군 차장 패트릭 쥐스텔 장군은 나토가 외국 시스템을 별다른 의심 없이 받아들이는 관행이 자국의 정보 안전을 위협한다고 지적했습니다. 프랑스와 독일 정상은 2026년 7월 17일, 유럽 자체의 주권적 디지털 백본을 만들겠다는 공동선언에 서명했습니다.

아르카디아가 메이븐 스마트 시스템을 대체할 수 있을 만큼 자리 잡으려면 시간이 걸립니다. 그동안 나토 지휘 체계의 상호운용성 요구는 회원국이 표적 정보를 공유하고 통신 표준을 맞추도록 계속 압박할 것이고, 그 압박은 이미 검증받고 표준을 충족한 팔란티어의 시스템 쪽으로 조달을 끌어당깁니다. 국내 정보기관은 국경 안에서 결정을 내리고 계약을 끝낼 수 있지만, 서른두 개 나라가 함께 쓰는 지휘 체계는 한 나라가 마음대로 바꿀 수 없습니다. 이 차이가 나토 안에서 상호운용성이 국내 통제권을 계속 압도하는 이유입니다.

근거자료

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 공식 보도자료, 2026년 6월 30일.

3. Tamara Rozouvan, 'Maven Smart System achieves full operating capability with NATO', Janes, 2026년 7월 1일.

4. 누라이 테일러, 'NATO's 'Digital Lethality Branch' Breaks Records in Drive for Alliance-Wide Interoperability', AFCEA International, 2026년 7월 31일.

5. 페르난도 카스트로 데 베이로, 'Foreign software, Europe's War: How Maven and Palantir are already making decisions for Europe', DigitalShield, 2026년 7월 15일.

6. 위키백과(Wikipedia), 'Palantir', 2026년 8월 9일 최종 개정.

7. 기자 미상, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026년 8월 3일.

8. Egl Kri topaityt, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, 2026년 7월 2일.

9. T.Wiegold, 'Cyber-Kommandeur der Bundeswehr lehnt Software von Palantir ab', Augen geradeaus!, 2026년 4월 28일.

10. Cybernews 편집국, 'France and Germany to build an alternative to Palantir', Cybernews, 2026년 7월 20일.

11. 존 헨리, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026년 6월 16일.

12. 저자 미상, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, 2026년 5월 26일.

3.3 유럽연합 인공지능법(AI Act) 안보 예외 조항과 통제의 사각지대

인공지능법(AI Act)은 인공지능 시스템이 사람에게 미칠 수 있는 위험의 크기에 따라 규제 강도를 달리하는 법입니다. 위험이 큰 시스템일수록 투명성과 위험 평가, 인간의 감독 의무를 무겁게 지웁니다. 이 규정 제2조는 군사, 국방, 국가안보 목적으로만 시장에 나오거나 사용되는 인공지능 시스템에는 이 법이 적용되지 않는다고 정합니다. 이 예외는 시스템을 만들거나 운용하는 주체가 정부 기관인지 민간 기업인지를 가리지 않습니다. 리사이틀(전문) 24는 그 근거를 밝힙니다.

국가안보는 유럽연합 조약 체계 안에서 회원국이 단독으로 책임지는 영역이고, 군사와 국방 활동은 그 성격상 유럽연합의 공동외교안보정책 아래 별도의 규율을 받는다는 것입니다.

이 예외 조항은 협상 과정에서 우연히 남은 틈이 아니라 회원국들이 적극적으로 요구해 얻어낸 결과입니다. Centre for Future Generations의 2026년 봄호 보고서에 따르면, 프랑스는 이탈리아, 스웨덴과 함께 국가안보를 근거로 예외 범위를 넓히자는 로비를 이끌었습니다. 이들 정부는 치안 당국이 공공장소에서 얼굴 인식 카메라나 생체 인식 감시 도구를 쓸 때 브뤼셀의 위험 평가 절차를 거치지 않아도 되기를 원했습니다. 그 결과 국내 치안 기관의 정보망과 군사 동맹의 표적 식별 시스템은 나란히 인공지능법의 적용 범위 밖으로 나갔습니다.

이 사각지대 안에 놓인 대표적인 시스템이 국내 치안용 고섬 계열 프로그램과 나토의 메이븐 스마트 시스템입니다. 인공지능법이 다른 고위험 시스템에 요구하는 문서화 의무, 오작동과 편향을 추적하는 절차, 사람이 최종 결정을 검토하는 장치는 이 두 시스템에는 법적으로 강제되지 않습니다. 나토 보안인증위원회가 2026년 6월, 메이븐 스마트 시스템에 완전 운용 인증을 내린 절차는 이 법의 심사를 거치지 않았습니다.

그러나 이 면제는 무규제와 같은 말이 아닙니다. 제2조의 예외는 군사, 국방, 국가안보 목적으로만 쓰이는 경우에 한정됩니다. 같은 회사가 만든 같은 종류의 소프트웨어라도 공공행정이나 민간 치안 업무처럼 군사 목적이 아닌 곳에 쓰이면 인공지능법의 적용을 받습니다. 예외는 특정 기업이나 특정 고객에게 붙는 표가 아니라, 그 인공지능이 실제로 쓰이는 용도에 붙는 조건입니다.

인공지능법이 비켜간 자리에 다른 법적 장치가 전혀 없는 것도 아닙니다. 독일 연방헌법재판소는 2023년 2월 16일, 인공지능법이 만들어지기도 전에 헤센주 경찰의 자동 데이터 분석 시스템 헤센데이터에 위헌 결정을 내렸습니다. 이 판결은 국가안보나 치안을 명분으로 삼은 인공지능 시스템이라도 각국의 헌법 질서 안에서는 별도의 법적 근거를 갖춰야 한다는 원칙을 세웠습니다. 인공지능법의 국가안보 예외는 이 규정 하나가 적용되지 않는다는 뜻일 뿐, 회원국의 헌법과 개인정보 보호 법령, 의회의 감독 권한까지 모두 사라진다는 뜻은 아닙니다.

나토 차원에서도 완전한 무법 지대는 아닙니다. 메이븐 스마트 시스템이 나토 보안인증위원회의 승인을 거쳐야 했다는 사실 자체가, 인공지능법이 비켜간 자리에 나토 고유의 인증 절차가 대신 들어와 있다는 뜻입니다. 다만 이 인증 절차는 시스템이 안전하게 작동하는지를 군사적 기준에서 확인하는 절차이지, 인공지능법이 요구하는 편향 점검이나 시민에 대한 투명성 의무와 같은 기준으로 설계되지 않았습니다. 감독의 주체와 기준이 바뀌었을 뿐, 감독 자체가 사라진 것은 아닙니다.

다만 그 감독이 국방 기밀 아래 놓이면서, 시민이 그 결과를 들여다볼 통로는 국내 정보 영역에 비해 훨씬 좁아졌습니다.

유럽의회는 2026년 1월, 미국의 소수 기술 기업에 대한 의존을 줄이자는 기술주권 결의안을 표결에 부쳐 가결했습니다. 의원들은 마이크로소프트와 아마존 같은 미국 기업에 데이터가 지나치게 몰리면, 미국 정부의 결정 하나로 유럽의 서비스가 멈출 수 있다는 위험을 근거로 들었습니다. 미국 행정부는 이런 유럽의 규제 움직임에 반발하며 무역 보복 가능성을 내비쳤습니다.

프랑스와 독일 정상은 2026년 7월 17일, 유럽 자체의 주권적 디지털 백본을 만들자는 공동선언에 서명했습니다. 이 선언이 가리키는 방향은 아르카디아 같은 자체 소프트웨어를 실제로 완성하는 일입니다. 인공지능법의 국가안보 예외는 유럽이 미국 기술에 의존하는 상태를 규제로 막을 수 없다는 사실을 인정한 조항이지, 그 의존을 해결하는 조항은 아닙니다. 규제의 손이 닿지 않는 자리를 채우는 일은 유럽이 스스로 만든 대안 기술의 몫으로 남았습니다.

근거자료

1. Regulation (EU) 2024/1689, Artificial Intelligence Act, Article 2 and Recital 24, 2024년 12월 13일.

2. Centre for Future Generations, 「Enforcement spotlight - Spring 2026」, Centre for Future Generations, 2026년 봄호, 2-3쪽.

3. 독일 연방헌법재판소, 'Decisions search - Judgment of 16 February 2023', 독일 연방헌법재판소, 2023년 2월 16일.

4. 프랑스 상원 조사위원회, '유럽연합(EU) 주요국의 탈(脫)팔란티어 행보와 디지털 주권화에 관한 분석 보고서', 프랑스 정부 공식 포털, 2026.

5. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE 공식 보도자료, 2026년 6월 30일.

6. 네덜란드 국방부 및 유럽 기술 위원회, '유럽의 팔란티어 이탈 흐름을 원 소스까지 확인해 정리한 자료', 2026.

제4장. 유럽의 반격: 기술주권 패키지와 CADA의 4단계 프레임워크

4.1. 클라우드·AI 개발법(CADA)과 데이터 센터 가속화 구역의 규제 혁신

유럽연합 집행위원회는 2026년 6월 3일 클라우드·AI 개발법 제안을 정식으로 내놓았다. 영어 이름은 Cloud and AI Development Act, 줄여서 CADA라 부른다. 문서 번호는 COM(2026) 502다. 이 사실부터 분명히 해 두어야 한다. CADA는 아직 법률이 아니다. 유럽연합 집행위원회가 유럽의회와 이사회에 심의를 요청한 규정 제안이며, 이 책이 다루는 2026년 8월 11일 시점까지 정식으로 채택되지 않았다.

유럽연합에서 규정(Regulation)은 지침(Directive)과 달리 회원국 의회의 별도 입법 없이 곧바로 효력을 갖는 강한 법 형식이다. 그만큼 규정으로 확정되기까지의 심의 절차도 무겁다. 일반입법절차에서는 유럽의회와 이사회가 각각 수정안을 내고 표결을 거친 뒤에야 조문이 확정된다. 그 과정에서 지금 제안서에 담긴 조문과 수치는 달라질 수 있다. 이 장에서 설명하는 4단계 주권 보증 수준과 가속화 구역, 해지권 조항은 모두 제안 단계의 설계도다. 이미 회원국 정부와 기업을 구속하는 규범이 아니다.

이 구분은 유럽연합 인공지능법(AI Act, Regulation (EU) 2024/1689)과 CADA를 혼동하지 않기 위해서도 필요하다. 인공지능법은 2024년에 이미 제정되어 효력을 갖고 있는 규정으로, 인공지능 시스템을 위험도에 따라 분류하고 그에 맞는 의무를 부과하는 법이다. 반면 CADA는 그 인공지능이 돌아갈 인프라와 조달 절차를 다루는 별도의 제안이며, 2026년 8월 현재 아직 제정되지 않았다. 두 법의 이름에 나란히 인공지능이라는 단어가 들어가 있다는 이유로 두 법의 법적 지위를 같은 것으로 취급해서는 안 된다.

하나는 이미 시행 중인 규범이고, 다른 하나는 아직 심의를 기다리는 제안이다.

CADA는 집행위원회가 추진해 온 인공지능 대륙 행동계획의 한 부분으로 등장했다. 계획의 목표는 두 가지로 요약된다. 유럽 안에 있는 데이터센터의 연산 능력을 늘리는 일과, 그 연산 능력을 유럽 바깥의 사법 관할로부터 지키는 일이다. 이 두 목표가 하나의 법안 안에 묶인 배경에는 유럽 클라우드 시장의 구조가 있다. 아마존과 마이크로소프트, 구글 세 회사가 유럽 클라우드 인프라 서비스 시장에서 압도적인 비중을 차지하고 있고, 유럽에 본사를 둔 기업들의 몫은 그에 크게 못 미친다고 여러 업계 보고서가 전한다.

기술정책 매체 테크폴리시프레스는 2026년 6월 15일 기사에서 이런 쏠림이 공공 시스템의 운명을 외국의 사법권 아래 두는 안보 취약점으로 이어진다고 지적했다.

CADA 이전에도 유럽은 비슷한 시도를 한 적이 있다. 2019년 프랑스와 독일이 주도해 시작한 가이아엑스(Gaia-X)는 유럽 기업들이 공동으로 쓸 수 있는 데이터 인프라 표준을 만들려던 민간 주도 프로젝트였다. 그러나 가이아엑스는 법적 구속력이 없는 자발적 협의체였고, 참여 기업들 사이의 이해관계가 엇갈리면서 애초에 목표했던 만큼의 성과를 내지 못했다는 평가를 받았다. CADA가 가이아엑스와 다른 점은, 자발적 표준이 아니라 법적 구속력을 가진 규정으로 조달 시장 자체를 움직이려 한다는 데 있다.

다만 그 규정이 실제로 힘을 가지려면 유럽의회와 이사회의 심의를 통과해야 한다는 점에서, CADA 역시 아직은 의지의 표명 단계에 머물러 있다.

일반 독자에게는 낯선 이야기일 수 있다. 정부나 병원, 경찰이 쓰는 컴퓨터 시스템이라고 해서 반드시 그 나라 국경 안의 건물에서 돌아가는 것은 아니다. 아마존이나 마이크로소프트, 구글 같은 회사의 클라우드 서비스를 빌려 쓰면, 실제 연산은 그 회사가 세계 곳곳에 지어 놓은 대형 서버 단지에서 이뤄진다. 이런 초대형 서버 단지를 업계에서는 하이퍼스케일러라 부른다. 서버 건물이 물리적으로 유럽 땅 위에 있어도, 그 건물을 소유하고 운영하는 회사가 미국 법인이라면 미국 정부의 법적 요구가 그 위의 데이터에 미칠 수 있다.

물리적 위치와 법적 통제권이 다를 수 있다는 이 간극이 이 장 전체를 관통하는 핵심 논점이다.

여기에 더해 클라우드 산업에는 데이터 중력이라 불리는 현상이 있다. 한 번 대량의 데이터를 특정 회사의 클라우드에 옮겨 놓으면, 그 데이터를 처리하는 다른 프로그램과 서비스도 같은 클라우드 안에 함께 놓는 편이 빠르고 저렴해진다. 시간이 지날수록 데이터와 그 데이터를 다루는 응용 프로그램이 한 회사의 생태계 안으로 점점 더 깊이 얽혀 들어간다는 뜻이다. 공공기관이 처음에는 저장 공간을 빌리는 정도로 계약을 시작했다가, 몇 해 지나지 않아 행정 업무 전체가 한 회사의 클라우드 없이는 돌아가지 않는 상태에 이르는 일이 드물지 않다.

유럽의 정책 입안자들이 시장 점유율 수치보다 이 얽힘의 깊이를 더 걱정하는 이유가 여기에 있다.

마리오 드라기 전 유럽중앙은행 총재가 2024년 9월 유럽연합에 제출한 경쟁력 보고서는 이 문제를 미리 경고한 문서로 자주 인용된다. 드라기 보고서는 유럽이 독자적으로 인공지능을 개발하고 서비스를 운영하려면 주권이 보장된 연산 처리 능력을 갖춰야 한다고 권고했다. 이 권고는 이후 유럽연합 집행위원회의 정책 문서 곳곳에 되풀이해서 등장한다. 유럽 안에 서버를 두었다는 사실만으로는 부족하다는 인식, 그 서버를 통제하는 기업의 국적과 지배 구조까지 따져야 한다는 인식이 CADA 제안의 출발점이다.

집행위원회는 이 데이터센터 확충 목표를 인공지능 기가팩토리라는 이름의 별도 사업과 함께 묶어 추진하고 있다. 인공지능 기가팩토리는 대규모 그래픽처리장치 클러스터를 갖춘 초대형 연산 시설을 가리키는 이름으로, 인공지능 대륙 행동계획에서 제시된 개념이다. 서버 대수를 늘리는 데서 그치지 않고, 유럽 안에서 대형 인공지능 모델을 처음부터 끝까지 훈련시킬 수 있는 연산 능력을 확보하겠다는 목표가 이 사업의 배경에 있다. 지금까지 유럽의 연구자와 기업들은 대형 모델을 훈련시키려면 미국 클라우드 회사가 제공하는 연산 자원을 빌려 써야 했다.

CADA와 인공지능 기가팩토리는 이 임대 구조 자체를 바꾸려는 시도다.

이 목표를 뒷받침하는 인프라가 이미 일부 가동되고 있다는 점도 짚어 둘 만하다. 유럽연합은 2018년부터 유로 고성능컴퓨팅 공동사업(EuroHPC Joint Undertaking)을 통해 회원국과 함께 슈퍼컴퓨터를 운영해 왔다. 핀란드의 루미(LUMI)나 스페인의 마레노스트룸(MareNostrum) 같은 기존 슈퍼컴퓨터를 인공지능 훈련용 연산 자원으로 전환하는 사업이 CADA 발의보다 앞서 이미 시작됐다.

CADA와 인공지능 기가팩토리 구상은 이 기존 자산을 완전히 대체하는 것이 아니라, 그 위에 민간 자본과 회원국 예산을 더 끌어들여 규모를 키우는 방향으로 설계됐다.

집행위원회가 밝힌 CADA의 수치 목표는 명확하다. 유럽연합의 데이터센터 역량을 앞으로 5년에서 7년 사이에 세 배 이상으로 늘리겠다는 것이다. 그렇게 늘어난 역량으로 2035년까지 기업과 공공행정의 수요를 충족하겠다는 목표다. 이 목표는 집행위원회가

발행한 제안 문서 자체에 담겨 있다. 목표가 이렇게 크게 잡힌 이유는 수요와 공급의 간극이 이미 벌어지고 있기 때문이다.

유럽의회가 2026년 1월 22일 채택한 「유럽 기술주권과 디지털 인프라」 문서는 전 세계 전력 소비의 상당 부분이 데이터센터와 통신 설비에서 발생하고 있으며, 유럽 데이터센터의 전력 소비 비중이 앞으로 몇 년 사이 눈에 띄게 늘어날 것으로 내다봤다. 인공지능 연산이 본격적으로 늘어나면 이 비중은 한층 가팔라진다. 데이터센터를 짓는 속도가 그 수요를 따라가지 못하면, 유럽은 인공지능 개발에서 미국이나 중국의 클라우드를 빌려 쓰는 처지를 벗어나기 어렵다.

문제는 데이터센터를 짓는 일 자체가 느리다는 데 있다. 회원국 안에서 공공 행정용 데이터 저장 시설을 새로 세우려 할 때마다 복잡한 인허가 절차와 토지 규제, 환경영향평가가 사업의 발목을 잡는 사례가 거듭 보고됐다. 독일 연방정보기술보안청과 국제 법무법인 버드앤버드가 2026년 4월 27일 함께 낸 보고서는 독일 연방정부와 주 정부 사이의 행정 절차 불일치가 조달 규격서 단계에서부터 지연을 낳고 있다고 지적했다. 이런 지연은 독일만의 문제가 아니다.

대규모 클라우드 서버 구축 계획이 지역 주민의 반발이나 환경 심사 지연 때문에 축소되거나 무산되는 일은 유럽 여러 나라에서 되풀이돼 왔다. 한 지역에서 데이터센터 부지를 정하고 전력을 끌어오고 인허가를 받는 데만 여러 해가 걸리는 사이, 연산 수요는 그보다 훨씬 빠른 속도로 불어난다.

CADA 제안은 이 지연을 줄이기 위한 절차 혁신을 핵심 축으로 삼는다. 정치 매체 폴리티코 유럽판은 2026년 6월 4일 보도에서 CADA가 회원국 정부에 지리와 전력망 조건이 좋은 부지를 데이터센터 가속화 구역으로 지정하도록 권한다고 전했다. 법무법인 버드앤버드가 정리한 기술주권 패키지 개요 보고서 역시 이 가속화 구역 안에서는 인허가 절차가 단일 창구로 통합되고, 처리 기한에 상한이 설정된다는 제안의 취지를 확인했다. 사업자가 여러 관청을 따로 찾아다니는 대신 한 곳에서 사업의 전체 생애주기를 조율받는 방식이다. 이 단일 창구가 통합하려는 절차는 다양하다.

전력망 연결 승인, 상수도와 냉각수 공급 허가, 건축 안전 심사, 통신 회선 인입 허가처럼 서로 다른 관청이 따로 관리하던 절차를 하나의 창구에서 조율하겠다는 것이다. 지금까지는

사업자가 이 절차들을 하나씩 순서대로 밟아야 했고, 한 단계에서 지연이 생기면 뒤이은 절차 전체가 밀리는 구조였다. 보도에 따르면 이 가속화 구역 안에서는 기밀 데이터를 다루는 시설의 인허가 처리 기한이 최대 18개월로 제한된다.

대형 시설 하나를 짓는 데 필요한 인허가 절차가 여러 해씩 걸리는 사례가 드물지 않았다는 점을 생각하면, 이 상한선은 절차 자체를 근본적으로 다시 짜겠다는 신호로 읽힌다.

환경영향평가 절차 역시 가속화 구역 안의 사업에 한해 간소화되는 방향으로 설계됐다고 같은 보고서는 전한다. 이 간소화가 실제로 환경 심사 자체를 면제하는 수준인지, 심사 기간만 줄이는 수준인지는 제안서가 유럽의회와 이사회의 심의를 거치며 구체화될 사안이다. 지금 단계에서 확정된 조문으로 단정하기는 이르다. 다만 그 방향성만큼은 뚜렷하다. 국가 안보와 직결되는 인프라 사업이라면, 통상적인 지방자치 인허가 절차보다 우선순위를 둔다는 것이다.

부지를 가속화 구역으로 지정하는 권한은 일차적으로 회원국 정부에 있다고 알려져 있다. 지방정부나 중앙정부가 전력망 여유 용량과 통신 회선 접근성, 물리적 보안이 확보되는 부지를 추려 집행위원회에 제안하면, 집행위원회가 이를 검토해 최종 목록에 반영하는 방식이다. 이 절차는 반도체법이 이미 시행하고 있는 파운드리 부지 지정 방식과 비슷한 틀을 빌려 왔다고 평가된다.

이 확충 목표는 유럽연합의 기후 목표와도 맞물린다. 유럽연합은 2050년까지 탄소중립을 이루겠다는 목표를 유럽 그린딜을 통해 못박아 두었다. 데이터센터 전력 소비가 계속 늘어나는 상황에서 이 목표를 지키려면, 새로 짓는 시설의 상당수를 재생에너지로 가동해야 한다는 압박이 뒤따른다. CADA가 가속화 구역의 특혜를 지속가능성 기준과 연결한 것은, 속도를 위해 기후 목표를 희생하지 않겠다는 신호로 읽을 수 있다.

가속화 구역 구상에는 위험도 따라붙는다. 절차를 빨리 통과시켜 주는 특혜는 그 특혜를 받는 사업이 실제로 공익에 부합하는지 검증하는 장치가 없으면 세금 낭비로 이어질 수 있다. 스웨덴에서는 2022년 정부가 자국의 기술 인프라를 확충하려는 목적으로 데이터센터 기업에 세제 혜택을 지급했는데, 그 기업들이 재생에너지 사용 계획을 실제로 지켰는지 검증하는 절차가 미비했다는 지적이 뒤따랐다. 스웨덴 매체 시큐리티유저닷컴은 2026년 3월 이 문제를 되짚으며 북유럽 각국이 디지털 주권 인프라 정책을 다시 설계하고

있다고 전했다.

CADA 제안은 이런 실패를 되풀이하지 않기 위해 가속화 혜택을 받는 사업자에게 지속가능성 기준 준수를 증명하도록 요구하는 안전장치를 포함하고 있다고 버드앤버드 보고서는 설명한다. 속도를 위해 절차를 줄이되, 그 대가로 결과를 검증하는 의무를 새로 얹은 셈이다.

재정 규모를 보면 CADA가 홀로 움직이는 법안이 아니라는 사실이 드러난다. 집행위원회가 2026년 6월 3일 함께 공개한 부속 문서(COM(2026) 555 final/2)는 클라우드·AI 개발법과 차세대 안보 패키지를 완전히 실행하는 데 2036년까지 총 3,000억 유로에 이르는 투자가 필요하다고 추산했다. 이 가운데 데이터센터 인프라 확충에 2,000억 유로가 배정된다. 반도체 파운드리와 인공지능 기가팩토리 구축에는 1,000억 유로가 추가로 배정될 것으로 이 문서는 전망했다.

이 투자 계획은 클라우드·AI 개발법 하나만을 위한 것이 아니다. 2023년 발효된 유럽연합 반도체법이 반도체 생산 능력 확충을 다뤘다면, CADA의 재정 계획은 그 반도체 위에서 돌아갈 데이터센터와 인공지능 인프라를 다루는 후속 사업에 가깝다. 업계 분석 보고서 innobu는 이 두 법이 함께 묶여 유럽의 기술주권 패키지를 이룬다고 설명했다. 이 수치는 어디까지나 집행위원회의 추산이며, 실제 집행 예산은 회원국과 유럽의회의 예산 협상을 거쳐야 확정된다.

유럽연합 정상들이 2025년 11월 18일 베를린에 모여 안보 회담 공동선언을 발표한 일이 이 재정 계획의 정치적 배경으로 거론된다.

이 인프라 확충이 다루는 위협의 성격은 제2장에서 살펴본 모델 접근 차단과는 결이 다르다. 앤트로픽이 페이블 5에 대한 외국인 접근을 일시 중단했던 사건은 소프트웨어 계층에서 벌어진 일이었다. 미국 정부의 수출통제 지시 하나로 특정 모델에 대한 접근 권한 자체가 막혔다. 반면 데이터센터를 소유하지 못한 상태에서 발생하는 위협은 더 근본적이다. 연산 능력 자체를 다른 나라의 기업에 빌려 쓰는 처지라면, 모델이 아니라 그 모델이 돌아가는 하드웨어에 대한 접근이 막힐 수 있다는 뜻이다. CADA가 겨냥하는 것은 이 하드웨어 층위의 취약성이다.

버드앤버드와 IT 매체 잇벨트의 보도를 종합하면, CADA 제안은 2030년까지 유럽 역내 민간 기업의 상당수가 주권 클라우드 서비스로 이전하도록 유도하는 목표치도 함께 제시했다고 한다. 아울러 저지연 에지 컴퓨팅 거점을 대륙 전역에 촘촘히 배치해, 미국 대형 플랫폼에 대한 의존을 소비자 서비스 영역에서도 낮추겠다는 구상이 함께 거론된다. 이 목표들이 최종 규정에서 강제 의무로 남을지, 권고 수준으로 완화될지는 심의 과정을 지켜봐야 한다.

이 우선순위 지정에는 지역 사회의 발언권이 줄어드는 대가가 따른다. 데이터센터가 국가적으로 중요한 전략 사업으로 지정되면, 그 부지의 주민들이 통상적인 도시계획 절차에서 행사할 수 있었던 이의 제기나 공청회 참여의 폭이 좁아질 수 있다. 속도를 위해 절차를 줄인다는 것은, 그 절차 안에 있던 지역 주민의 목소리를 줄인다는 뜻이기도 하다. 이 균형을 CADA가 최종적으로 어떻게 조정할지는 아직 확정되지 않았다.

전력 확보 방식을 놓고 회원국 사이의 접근도 갈린다. 원자력 발전 비중이 높은 프랑스는 원자력 발전소 인근에 데이터센터를 짓는 방안을 정책적으로 밀어붙이고 있다. 안정적인 저탄소 전력을 데이터센터에 바로 공급할 수 있다는 것이 이 접근의 장점으로 꼽힌다. 반면 재생에너지 중심으로 전력망을 재편해 온 나라들은 태양광과 풍력의 간헐성을 데이터센터의 24시간 가동 수요와 어떻게 맞출 것인지를 별도로 풀어야 한다. CADA의 가속화 구역 지정 기준에 전력망 조건이 포함된 것도 이런 나라별 사정 차이를 고려한 설계로 보인다.

가속화 구역 지정이 특정 회원국에 집중될 가능성도 논의된다. 전력망과 통신 인프라가 이미 잘 갖춰진 서유럽과 북유럽의 일부 지역이 먼저 지정 요건을 충족할 공산이 크고, 기반 시설 투자가 상대적으로 더딘 동유럽과 남유럽 일부 지역은 뒤처질 위험이 있다. 유럽연합의 지역 균형 발전 원칙과 데이터센터 가속화라는 속도의 논리가 어떻게 조화를 이룰 것인지도, CADA가 최종 조문을 다듬는 과정에서 다뤄야 할 과제로 남아 있다.

CADA가 그리는 그림은 결국 하나의 질문으로 좁혀진다. 유럽이 자기 데이터를 저장할 물리적 공간을 스스로 짓지 못하면, 그 위에서 돌아가는 소프트웨어의 주권을 논하는 일도 공허해진다는 것이다. 물리적 데이터센터라는 토대 위에는 또 하나의 층이 있다. 누가 그 데이터센터를 통제하는가를 가르는 기준이다.

근거자료

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, 2026년 6월 15일, https://www.techpolicy.press/does-europe-really-have-a-plan-for-tech-sovereignty-cada/

4. Mario Draghi, 「The Future of European Competitiveness」, European Commission, 2024년 9월.

5. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', 유럽의회 관보, 2026년 1월 22일.

6. 독일 연방정보기술보안청, 「Digitale Souveränität bei IT-Vergaben: Zwischen politischem Anspruch und vergaberechtlicher Wirklichkeit」, Bird & Bird Insights, 2026년 4월 27일.

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

8. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, 2026년 6월 23일.

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

10. European Commission, COM(2026) 555 final/2, 유럽연합 관보, 2026년 6월 3일.

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

12. Itwelt 편집국, 'Best European cloud alternatives: Top 10 of 2026', Itwelt, 2026년 2월.

4.2. CADA의 4단계 주권 보증 수준(Sovereignty Assurance Levels) 설계

CADA 제안이 세운 두 번째 축은 데이터센터라는 물리적 껍데기가 아니라 그 안에서 도는 소프트웨어와 그것을 운영하는 기업의 국적을 가리는 기준이다. 집행위원회는 이 기준을 네 단계로 나누어 제시했다. 영어로는 소버린티 어슈어런스 레벨(Sovereignty Assurance Level), 줄여서 SEAL이라 부른다. 런던의 안보 정책 연구기관 블룸즈버리 정보안보연구소(BISI)가 2026년 7월 7일 낸 보고서는 이 네 단계 구조를 CADA의 세 축 가운데 하나로 정리하면서, 그 설계 목적이 미국 클라우드법(CLOUD Act)과 해외정보감시법 702조가 유럽 공공 데이터에 미치는 영향력을 차단하는 데 있다고 설명했다.

미국 의회가 2018년 통과시킨 클라우드법은 미국 법인이 경영을 지배하는 정보통신 서비스 사업자에게, 데이터가 어느 나라에 저장돼 있는지와 무관하게 수사기관에 자료를 보존하고 제출할 의무를 지운다. 법안 본문과 의회 요약에서 확인되는 이 조항은 유럽 안에 세워진 미국 기업의 자회사에도 적용될 수 있다. 유럽 기업과 계약을 맺고, 유럽 영토 안에 서버를 두고, 유럽의 개인정보보호법을 지킨다 해도, 그 서버를 운영하는 회사의 모기업이 미국 법인이라면 미국 수사기관의 요청이 계약서보다 우선할 수 있다는 뜻이다.

집행위원회가 CADA 제안과 함께 낸 부속 실무 문서(SWD(2026) 502 final)는 이 역외 관할권 문제를 상세히 분석한 것으로 알려졌다.

SEAL 체계를 개인정보보호법과 혼동해서는 안 된다. 유럽연합의 일반정보보호규정(GDPR)은 개인정보를 어떻게 수집하고 처리해야 하는지를 규율하는 법이며, 이미 2018년부터 시행되고 있다. GDPR을 지킨다고 해서 그 정보를 다루는 회사의 국적 문제까지 해결되는 것은 아니다. 정보를 아무리 안전하게 암호화하고 필요한 만큼만 수집해도, 그 정보를 보관한 회사가 미국 법인이라면 미국 정부의 법적 요청 앞에서 GDPR의 보호는 한계를 드러낸다. GDPR이 규율하는 것은 정보를 다루는 방식이고, SEAL이 규율하려는 것은 그 정보를 다루는 회사의 국적과 지배 구조다.

두 법은 서로 다른 층위에서 같은 데이터를 바라본다.

유럽 법원은 이미 한 차례 이 문제와 정면으로 부딪힌 적이 있다. 유럽사법재판소는 2020년 7월 이른바 쉬렘스 투 판결에서, 미국 정보기관이 통신 데이터에 접근할 수 있는 미국의 감시 법제를 이유로 유럽연합과 미국 사이의 개인정보 이전 협정인 프라이버시 실드를 무효로 판단했다. 계약서에 아무리 개인정보 보호 조항을 촘촘히 넣어도, 그 계약의 상대방이 미국 법의 적용을 받는 한 미국 정보기관의 접근 가능성 자체를 계약으로 막을 수는 없다는 것이 이 판결의 요지였다.

CADA가 국적과 지배 구조라는, 계약 조항보다 훨씬 근본적인 기준으로 주권 등급을 나누기로 한 배경에는 이런 사법적 경험이 쌓여 있다. 유럽이 얻은 안보 교훈은 결국 계약서의 문구가 아니라 회사의 지배 구조와 국적이 실질적인 보호막이라는 사실이었다.

이 교훈은 시장의 반응으로도 이어졌다. 아마존과 마이크로소프트, 구글은 최근 몇 년 사이 유럽 고객을 겨냥해 저마다 이름을 붙인 주권형 클라우드 상품을 내놓았다. 데이터를 유럽 안에서만 저장하고 처리하며, 유럽인이 아닌 직원의 접근을 제한하겠다는 약속이 이런 상품들의 공통된 광고 문구다. 그러나 이런 상품이 SEAL의 상위 단계인 제3단계와 제4단계가 요구하는 지배 지분과 이사회 의결권까지 유럽에 넘기는 경우는 드물다. 서버의 위치와 운영 규정을 유럽화하는 것과, 회사의 소유권 자체를 유럽화하는 것은 전혀 다른 차원의 약속이다.

SEAL 체계가 하려는 일은 바로 이 두 차원을 구분해서 조달 기준에 명시하는 것이다.

구체적인 사례로 아마존웹서비스는 2023년 유럽 전용 법인을 따로 세워 유럽 시민으로 구성된 이사회와 경영진을 두는 유럽 주권 클라우드 사업을 발표했다. 데이터 저장과 운영 인력을 유럽 안에 두겠다는 약속이었다. 그러나 이 유럽 법인의 최종 지분은 여전히 미국의 모회사인 아마존닷컴이 쥐고 있다. SEAL의 제3단계와 제4단계가 요구하는 것은 바로 이 최종 지분 구조까지 유럽 소유로 바뀌는 것이므로, 이런 형태의 주권형 클라우드 상품은 하위 단계의 자격은 얻을 수 있어도 상위 단계의 문턱은 넘기 어렵다.

SEAL의 제1단계는 가장 기본적인 요건을 요구한다. 데이터의 저장과 처리가 유럽연합 영토 안의 시설에서 이루어져야 한다는 것이다. 이 단계는 국가 기밀성이 낮은 일반 행정 업무에 적용되며, 미국계를 포함한 역외 기업의 유럽 지사도 유럽 안에 데이터센터를 갖추고 있다면 이 기준을 충족해 입찰에 참여할 수 있다. 공급업체가 스스로 요건 충족을 선언하는

자율 증명 방식으로 승인이 이뤄지고, 별도의 제3자 감사는 요구되지 않는다.

제2단계는 데이터가 물리적으로 어디에 있는가를 넘어, 그 데이터를 다루는 소프트웨어의 공급망까지 들여다본다. 공급업체는 소프트웨어 구성 요소를 상세히 기록한 소프트웨어 자재명세서(SBOM)를 제출하고, 소스코드의 보안 취약점을 검증받아야 한다. 소프트웨어 자재명세서란 하나의 프로그램이 어떤 부품, 즉 어떤 외부 라이브러리와 오픈소스 구성 요소로 이루어져 있는지 낱낱이 적어 놓은 목록이다. 식품의 원재료 표시와 비슷한 개념이라고 생각하면 이해하기 쉽다.

어느 한 구성 요소에서 보안 결함이 발견됐을 때, 그 결함이 자신이 쓰는 시스템에도 들어 있는지 목록만 보고 빠르게 확인할 수 있어야 한다는 취지다. BISI 보고서에 따르면 이 단계는 의료 정보나 금융 인프라처럼 민감도가 중간 수준인 공공 서비스에 적용될 것으로 설계됐다. 역외 기업이라도 유럽 기업과 합작해 지배 구조를 나누고 기술적 격리 장치를 증명하면 이 단계의 자격을 얻을 수 있는 통로가 열려 있다.

제3단계부터는 요건이 눈에 띄게 엄격해진다. 데이터를 처리하는 공급 기업과 그 하청 기업의 본사가 유럽연합 영토 안에 실재해야 하고, 지배 지분과 이사회의 의결권이 유럽연합 국적자의 손에 있어야 한다. 시스템을 유지보수하는 핵심 인력 역시 유럽연합 국적을 가진 거주자여야 하며, 신원 조사를 통과해야 한다. 다만 집행위원회는 유럽연합과 정보 공유 조약을 맺고 사법 마찰이 없는 우방국에 대해서는 이 요건을 부분적으로 완화하는 예외 통로를 제안서에 남겨 두었다고 BISI 보고서는 전한다. 이 단계는 국가 치안 수사망이나 테러 위협 분석처럼 안보와 직결된 업무에 적용된다.

우방국 예외가 실제로 어떤 나라에 적용될지는 아직 확정되지 않았다. 정보 공유 조약과 사법 협력 체계를 유럽연합과 이미 갖춘 나라가 후보로 거론되지만, 구체적인 국가 명단은 제안서 단계에서 공개되지 않았다. 이 모호함은 CADA가 심의를 거치는 동안 가장 치열한 협상 대상이 될 대목 가운데 하나로 꼽힌다. 예외의 범위를 넓게 잡으면 제3단계의 실효성이 옅어지고, 좁게 잡으면 우방국과의 외교적 마찰을 감수해야 한다.

네 단계를 한꺼번에 떠올리기 어렵다면, 건물의 출입 통제를 떠올려 보면 된다. 로비는 방문증만 있으면 누구나 들어갈 수 있고, 사무실 층은 직원증이 있어야 들어갈 수 있고, 서버실은 별도의 승인을 받은 소수만 들어갈 수 있고, 가장 안쪽의 금고실은 신원 조회를

마친 극소수만 들어갈 수 있다. SEAL의 네 단계도 이와 비슷하게, 다루는 정보의 무게가 무거워질수록 접근을 허용받는 주체의 범위가 점점 좁아지는 구조다.

제4단계는 예외가 없는 단계다. 국방과 군사 기밀, 최상위 치안 분석처럼 국가의 존립과 직결되는 영역에 적용되며, 제3단계의 이사회 국적 요건과 인력 조건을 그대로 지키면서도 우방국에 대한 어떤 예외도 허용하지 않는다. 시스템의 설계 단계부터 소스코드의 유지보수에 이르기까지 외국 상업 자본이 관여할 여지를 원천적으로 차단한다. 공급업체는 유럽연합 사이버보안청(ENISA)이 발급하는 유럽 사이버보안 인증체계(EUCS)에서 최고 등급인 하이(High) 등급을 취득해야 입찰에 참여할 수 있다. 이 EUCS 인증체계는 CADA가 처음 만든 것이 아니다.

ENISA는 이미 여러 해 전부터 이 인증체계를 준비해 왔는데, 최고 등급에 비유럽 기업의 소유 지분을 제한하는 조항을 넣을 것인지를 두고 회원국 사이에 이견이 이어져 온 것으로 알려져 있다. 프랑스를 비롯한 일부 회원국은 소유 지분 제한을 강하게 요구했고, 다른 회원국은 그런 제한이 시장 경쟁을 해친다고 반대해 왔다. CADA가 제4단계 요건에 EUCS 하이 등급을 명시적으로 끌어들인 것은, 그동안 인증체계 안에서 결론을 내지 못했던 소유권 논쟁에 법적 무게를 더하려는 시도로 읽힌다.

BISI 보고서는 이 네 단계가 실제 공공 조달에서 어떤 비율로 적용될지에 관한 추산도 제시했다. 전체 공공 기술 도입 사업 가운데 약 70퍼센트에 이르는 민감도가 낮은 일반 행정 업무가 제1단계로 분류된다. 20퍼센트에 이르는 중간 민감도 업무는 제2단계로 분류된다. 나머지 10퍼센트는 제3단계와 제4단계로 나뉘는데, 9퍼센트가 제3단계로, 1퍼센트가 제4단계로 배정될 것이라고 이 보고서는 내다봤다. 이 추산은 아직 확정된 통계가 아니라 보고서의 분석에 기댄 전망이라는 점을 밝혀 둘 필요가 있다. 다만 이 비율이 시사하는 바는 뚜렷하다.

공공 조달의 절대다수는 여전히 제1단계와 제2단계에 머물고, 완전한 유럽 소유를 요구하는 제3단계와 제4단계는 전체 사업의 극히 일부에만 적용된다는 것이다.

이 단계별 설계는 완전히 새로운 발명이 아니다. 프랑스는 이미 자체 인증 체계인 섹넘클라우드(SecNumCloud)를 운영하며 국가 최고 등급의 보안 사용 사례에 미국 클라우드법의 영향력을 원천 차단하는 최상위 인증을 요구해 왔다. 이 인증은 프랑스

국가정보시스템보안청(ANSSI)이 관리하며, 최상위 등급을 받으려는 클라우드 사업자는 프랑스 또는 유럽연합 자본이 지배 지분을 갖추도록 요구받는다. BISI 보고서는 CADA의 4단계 구조가 이 프랑스식 인증 체계의 논리를 유럽연합 전체 층위로 확장한 설계라고 평가했다.

프랑스에서 이미 시행된 제도가 있었기에, CADA가 완전히 새로운 실험이 아니라 검증된 모델을 확장하는 제안이라는 설명이 성립한다.

프랑스의 섹넘클라우드 말고도, 몇몇 회원국은 저마다의 방식으로 독자적인 인증 체계를 발전시켜 왔다. 나라마다 기준이 다르면, 한 나라에서 인증받은 공급업체가 다른 나라의 조달에서는 처음부터 다시 심사를 받아야 하는 비효율이 생긴다. CADA가 단일한 SEAL 체계로 이 기준들을 통일하려는 이유가 여기에 있다. 스물일곱 개 회원국이 저마다 다른 인증 기준을 고집한다면, 유럽 전체를 아우르는 주권 클라우드 시장은 애초에 성립하기 어렵다.

승인 절차에서도 단계별로 무게가 다르다. 제1단계는 공급업체의 자율 증명만으로 통과되고, 중소기업에는 이중 서류 심사를 면제하는 간이 통로가 마련된다. 반면 제2단계부터 제4단계까지는 유럽연합이 지정한 독립적인 제3자 감사 기관이 시스템의 원천 설계도까지 정밀하게 검증한 뒤, 회원국의 전문 수사기관이 최종 승인을 내려야 한다. 한 회원국이 내린 승인 결정은 유럽연합 공동 등록부에 올라가고, 60일 동안 다른 회원국이 이의를 제기할 수 있는 상호 검증 기간을 거친다. 이 기간에 이의가 해소되지 않으면 집행위원회가 최종 조정안을 내려 분쟁을 정리하는 절차가 제안돼 있다.

한 나라가 내린 판단을 스물일곱 개 회원국 전체가 다시 들여다볼 수 있게 한 것은, 어느 한 나라의 느슨한 심사가 연합 전체의 보안 기준을 낮추는 구멍이 되지 않도록 막으려는 설계로 보인다.

인증은 한 번 받으면 끝나는 것이 아니다. 공급업체의 지분 구조나 이사회 구성이 바뀌면, 애초에 통과했던 SEAL 등급의 전제 자체가 무너질 수 있다. 유럽 기업으로 인증받았던 회사가 훗날 비유럽 자본에 인수된다면, 그 회사가 수행하던 공공 계약의 지위는 어떻게 되는가라는 질문이 남는다. BISI 보고서는 CADA가 이런 사후 변경을 감시하고 재심사하는 절차까지 포함하고 있다고 전하지만, 그 재심사가 얼마나 자주, 얼마나 신속하게

이뤄질지는 아직 구체화되지 않았다.

이 등급은 누가 정하는가라는 질문도 남는다. 공공기관이 새로운 사업을 조달에 부치기 전에, 먼저 그 사업이 다루는 데이터의 민감도를 스스로 진단하고 어느 SEAL 단계에 해당하는지 판정해야 한다. 일반 행정 문서를 다루는 사업이라면 제1단계로 분류되지만, 같은 기관이라도 치안이나 국방 정보를 다루는 사업이라면 제3단계나 제4단계로 분류될 수 있다. 이 판정이 잘못되면 뒤늦게 문제가 드러난다. 낮은 단계로 분류해 계약을 맺었다가 나중에 그 데이터가 국가 안보와 직결된다는 사실이 확인되면, 이미 맺은 계약을 다시 뜯어고쳐야 하는 상황에 몰린다.

CADA 제안이 판정 절차와 감사 체계를 함께 규정하려는 이유도 이 오분류 위험을 줄이기 위해서라고 이해할 수 있다.

인증 부담이 반드시 대기업에만 가벼운 것은 아니다. 제2단계부터 요구되는 소프트웨어 자재명세서 작성과 소스코드 검증에는 전담 인력과 비용이 들어간다. 자본력이 크지 않은 유럽의 신생 클라우드 기업들에는 이 부담이 시장 진입 자체를 가로막는 장벽으로 작용할 수 있다. CADA가 중소기업에 제1단계 간이 통로를 열어 준 것과 별개로, 성장 단계에 있는 유럽 기업이 상위 단계로 올라서도록 돕는 지원책이 함께 마련되지 않으면, 상위 단계의 시장은 결국 이미 자본을 갖춘 소수의 대기업에만 열리는 역설이 생길 수 있다.

이 네 단계 구조가 실제로 작동하려면 넘어야 할 산이 있다. 유럽 시장에는 아직 제3단계와 제4단계 요건을 충족할 만한 자국 기업의 공급 능력이 넉넉하지 않다는 것이 여러 업계 보고서가 공통으로 지적하는 문제다. 유럽 기업이 이 상위 단계 요건을 충족하는 데 시간이 걸리는 이유는 정치적 의지의 문제만이 아니다. 대형 클라우드 서비스를 운영하려면 서버 하드웨어와 네트워크, 냉각 설비에 막대한 초기 투자가 필요하고, 그 투자를 회수하려면 오랜 시간에 걸쳐 안정적인 고객군을 확보해야 한다.

미국의 대형 클라우드 회사들은 이미 수십 년에 걸쳐 이 투자와 회수의 순환 고리를 만들어 왔다. 유럽 기업이 이 순환 고리를 짧은 기간 안에 따라잡으려면, CADA가 정한 등급 기준만으로는 부족하고 그 등급을 채울 기업에 대한 별도의 자본 지원이 함께 움직여야 한다는 지적이 나온다. 요건을 아무리 정교하게 설계해도, 그 요건을 통과할 기업이 부족하면 공공기관은 결국 낮은 단계의 조달로 후퇴하거나 예외 조항에 의존하게 된다.

CADA가 정한 등급 자체보다, 그 등급을 채울 유럽 기업의 역량이 얼마나 빨리 자라는가가 이 제도의 실질적인 성패를 가를 변수로 남아 있다.

근거자료

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

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, 유럽연합 관보, 2026년 6월 3일, 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, 유럽연합 관보, 2026년 6월 3일.

5. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, 2026년 6월 23일.

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

4.3. '주권 사유 해지권(Sovereignty Termination Clause)'과 이식성 의무의 제도화

CADA가 아무리 정교한 등급을 설계해도, 이미 맺어진 계약을 어떻게 끝낼 것인가라는 질문에 답하지 못하면 그 등급은 새로 시작하는 사업에만 적용되는 반쪽짜리 제도로 남는다. 영국의 사례는 이 문제를 가장 선명하게 보여준다.

영국 국가보건서비스(NHS)는 2023년 팔란티어와 3억 3,000만 파운드 규모의 계약을 맺고 통합 데이터 플랫폼(Federated Data Platform)을 구축했다. 이 플랫폼은 영국 전역 병원의 환자 정보와 병상 현황, 대기 명단을 하나의 체계로 묶어 분석하는 시스템이다. 영국 하원 과학기술위원회는 이 계약이 국가 안보상 받아들이기 어려운 취약점이라고 경고하는 보고서를 냈다. 좌파 성향 매체 노바라 미디어는 여러 하원의원이 정부에 이 계약을 끝내라고 요구했다고 보도했다. 문제는 계약을 끝내고 싶어도 쉽게 끝낼 수 없다는 데 있었다.

하원 과학기술위원회 보고서에 따르면, NHS는 계약 기간 내내 이용료를 지불했음에도 시스템의 핵심 자산인 데이터 표준 모델(Canonical Data Model)과 온톨로지 지식재산권을 넘겨받지 못했다. 계약이 끝나는 순간 NHS의 손에 남는 것은 데이터가 아니라, 팔란티어의 소프트웨어 위에서만 작동하도록 짜인 데이터의 잔해였다. 이 계약에 담긴 사유 해지권 조항이 2027년 2월에야 발효한다는 사실도 하원 보고서를 통해 확인됐다. 계약을 정말로 끝내고 싶은 순간과, 실제로 끝낼 수 있는 법적 순간 사이에 몇 년의 간극이 있었던 셈이다.

공공 조달 계약에는 원래도 해지 조항이 있다. 계약 위반이 있을 때 해지하는 조항이나, 특별한 사유 없이 위약금을 물고 해지하는 임의 해지 조항이 흔히 쓰인다. CADA가 새로 도입하려는 것은 이 두 가지와 구별되는 세 번째 범주다. 공급업체가 계약을 성실히 이행하고 있어도, 그 공급업체의 국적과 지배 구조가 국가 안보에 위협이 된다고 판단되면 위약금 없이 계약을 끝낼 수 있는 근거를 별도로 마련하겠다는 것이다. 이런 사유가 법적으로 명확하게 정의되지 않으면, 반대로 공급업체가 자의적인 해지라며 소송을 제기할 여지도 함께 남는다.

이 사례가 드러내는 문제는 팔란티어라는 특정 회사에 국한되지 않는다. 공공기관이 특정 소프트웨어에 데이터를 맡기기 시작하면, 그 데이터는 점점 그 소프트웨어의 고유한 구조 안에서만 의미를 갖도록 길들여진다. 데이터를 다른 시스템으로 옮기는 일은 파일을 복사하는 것만으로 끝나지 않는다. 데이터가 담긴 분류 체계와 관계 구조, 즉 온톨로지 자체를 다시 설계해야 하는 경우가 많다. 온톨로지란 어떤 정보들이 서로 어떤 관계를 맺고 있는지를 정의한 설계도라 할 수 있다. 예를 들어 환자와 병상, 진료 기록이 어떻게 연결되는지를 정해 놓은 규칙 체계가 여기에 해당한다.

이 규칙 체계를 다른 회사의 시스템에 맞게 다시 짜는 작업에는 새로운 계약과 개발 인력, 상당한 예산이 든다. 계약 초기에는 저렴해 보였던 조달이 전환 시점에는 처음 계약보다 더 큰 비용을 요구하는 역설이 여기서 생긴다. 이런 구조적 잠금 효과를 업계에서는 흔히 벤더 락인(vendor lock-in)이라 부른다.

NHS 사례가 보여준 잠금 효과는 전통적인 데이터베이스에 국한되지 않는다. 인공지능 시대의 조달에서는 데이터뿐 아니라 그 데이터로 학습시킨 모델, 모델을 조정한 설정값, 검색에 쓰이는 임베딩까지 이전 대상에 포함된다. 공급업체가 이런 요소를 독점적인 형식으로 저장해 두면, 계약이 끝난 뒤 공공기관에 남는 것은 텅 빈 인프라뿐이고 그 위에 쌓아 올린 지능은 고스란히 공급업체의 손에 남는다. CADA의 이식성 의무가 실질적인 효과를 내려면, 이런 인공지능 특유의 자산까지 이전 대상에 포함하는 세부 규정이 필요하다는 지적이 나온다.

이식성을 기술적으로 보장하는 가장 흔한 방법은 개방형 표준을 쓰도록 강제하는 것이다. 데이터를 특정 회사만 읽을 수 있는 독점 형식이 아니라, 여러 시스템이 공통으로 읽고 쓸 수 있는 개방형 형식으로 저장하도록 계약서에 못박아 두면, 계약이 끝난 뒤에도 데이터를 다른 시스템으로 옮기는 작업이 상대적으로 수월해진다. 다만 개방형 표준을 쓴다고 해서 온톨로지처럼 그 시스템에 특화된 설계까지 자동으로 옮겨지는 것은 아니다. 데이터의 그릇을 개방형으로 바꾸는 일과, 그 그릇 안에 담긴 지식 구조를 옮기는 일은 서로 다른 과제로 남는다.

이식성이라는 개념이 유럽연합 법 안에 아예 없었던 것은 아니다. 2023년 채택된 유럽연합 데이터법(Data Act, Regulation (EU) 2023/2854)은 클라우드와 에지 컴퓨팅 서비스

사이의 전환을 다루는 조항을 이미 두고 있다. 이 법은 클라우드 이용자가 한 서비스 공급자에서 다른 공급자로 옮겨 갈 때 부과되는 전환 수수료를 단계적으로 낮추고, 정해진 시한 이후에는 이런 수수료 자체를 없애도록 정했다. CADA와 달리 데이터법은 이미 발효된 법이라는 점에서 차이가 있다.

CADA가 이 데이터법의 이식성 원칙을 공공조달이라는 훨씬 더 민감한 영역, 그리고 주권이라는 훨씬 더 무거운 기준으로 확장하려는 시도라고 이해하면, 두 법의 관계가 뚜렷해진다. 데이터법이 일반 상업 클라우드 이용자를 벤더 락인에서 지키려 했다면, CADA는 그 보호막을 국가 기관과 공공 서비스로까지 넓히려 한다.

CADA 제안이 다루려는 지점이 바로 이 대목이다. 집행위원회가 밝힌 정책 목표 가운데 하나는 공공기관이 주권상의 이유로 계약을 해지할 권리를 갖고, 공급업체는 계약 종료 시 데이터와 설정값을 개방되고 상호 운용이 가능한 형식으로 이전해 줄 의무를 진다는 것이다. BISI 보고서는 CADA의 세 축 가운데 하나가 이 이식성 의무의 제도화이며, 그 취지는 공공기관이 특정 공급업체에 발이 묶여 협상력을 잃는 상황을 막는 데 있다고 정리했다. 이 조항이 실제로 어떤 이름과 조문 번호로 최종 규정에 담길지는 유럽의회와 이사회의 심의를 거쳐야 확정된다.

지금 확인할 수 있는 것은 집행위원회가 이런 방향의 조항을 제안서에 담았다는 사실이지, 이미 시행 중인 규범이 있다는 사실이 아니다.

제안이 언급하는 전환 지원 기간이 구체적으로 어떤 모습일지는 아직 다듬어지지 않았지만, 비슷한 제도를 이미 시행 중인 다른 산업의 사례에서 짐작해 볼 수 있다. 통신 서비스 이용자가 번호를 그대로 유지한 채 통신사를 바꾸는 번호 이동 제도나, 은행 계좌를 옮길 때 자동이체 내역까지 함께 옮겨 주는 계좌 이동 제도가 그런 예다. 공공기관의 데이터 이식에도 이런 발상을 적용한다면, 옛 공급업체와 새 공급업체가 일정 기간 시스템을 나란히 운영하며 데이터와 업무를 단계적으로 넘기는 절차가 요구될 것으로 보인다.

이 제도가 성립하려면 두 가지가 함께 갖춰져야 한다. 하나는 법적으로 해지권을 명시하는 일이고, 다른 하나는 그 해지권을 실제로 행사할 수 있도록 기술적인 이식성을 확보하는 일이다. 법 조항만 있고 데이터 형식이 여전히 폐쇄적이라면, 공공기관은 계약을 끝낼 권리는 있어도 그 권리를 쓸 방법이 없다. 반대로 기술적으로는 데이터를 옮길 수 있어도

계약서에 위약금 조항이 걸려 있다면, 공공기관은 눈앞의 비용 때문에 낡은 시스템에 계속 머무르게 된다. NHS의 사례는 이 두 조건 가운데 어느 쪽도 충족되지 않았을 때 무슨 일이 벌어지는지를 보여주는 실패의 기록이다.

CADA가 실제로 시행된다 해도, 이미 맺어진 계약에 소급 적용될 것인지는 또 다른 문제로 남는다. 일반적으로 유럽연합의 새 규정은 시행일 이후에 새로 체결되는 계약에 우선 적용되고, 기존 계약에는 유예 기간이나 별도의 경과 조항이 따라붙는 경우가 많다. CADA 제안이 최종적으로 확정되는 과정에서 기존 계약에 대한 경과 규정을 어떻게 둘 것인지가 회원국 사이의 협상 쟁점이 될 가능성이 크다. 이미 여러 해째 특정 공급업체에 데이터를 맡겨 온 공공기관 입장에서는, 새 규정이 소급 적용되지 않는다면 이식성 의무의 효과를 체감하기까지 오랜 시간이 걸릴 수 있다.

계약을 처음 맺는 시점에는 이런 비용이 잘 보이지 않는다. 조달 담당자는 대개 초기 도입 비용과 연간 이용료를 기준으로 공급업체를 비교하고, 계약이 끝난 뒤 데이터를 빼내는 데 드는 비용까지 미리 계산에 넣는 경우는 많지 않다. 이 비대칭은 공급업체에도 나름의 유인을 만든다. 초기 가격을 낮게 제시해 계약을 따낸 뒤, 전환 비용을 높여 고객을 붙잡아 두는 전략이 클라우드 업계에서 드물지 않게 관찰된다는 것이 여러 시장 분석에서 지적돼 온 문제다. CADA의 이식성 의무는 이 유인 구조 자체를 계약 이전 단계에서부터 바꾸려는 시도로 볼 수 있다.

이 문제는 큰 나라보다 작은 나라에서 더 무겁게 나타난다. 인구가 많고 재정이 넉넉한 회원국은 계약을 검토할 전담 법률팀과 기술팀을 따로 꾸릴 여력이 있다. 반면 작은 회원국의 지방정부나 소규모 공공기관은 계약서를 검토할 전문 인력조차 충분하지 않은 경우가 흔하다. 공급업체가 제시하는 표준 계약서를 그대로 받아들이는 쪽이 협상에 매달리는 쪽보다 당장은 편하다. 이 비대칭이 쌓이면, 사유 해지권이 법전에 존재해도 그 권리를 실제로 행사할 역량을 가진 기관과 그렇지 못한 기관 사이에 격차가 생긴다.

CADA 제안이 중소기업 공급자에게 간이 승인 통로를 열어 준 것과 비슷한 논리로, 계약을 맺는 공공기관 쪽에도 표준화된 이식성 요건과 계약서 양식을 미리 마련해 주는 것이 협상력의 격차를 줄이는 길이라는 지적이 나온다.

전환 비용의 문제는 계약이 끝난 뒤에도 이어진다. 데이터를 옮기는 작업과 별개로, 그 데이터를 다루던 담당자들이 새 시스템을 익히는 데도 시간과 예산이 든다. 공공기관의 예산 주기는 대개 한 해 단위로 짜이기 때문에, 여러 해에 걸쳐 분산해서 들어가는 전환 비용을 한 번에 확보하기 어려운 경우가 많다. 이 때문에 사유 해지권이 법적으로 존재해도, 예산 부서가 전환 비용을 감당하지 못해 계약을 사실상 연장하는 사례가 여러 나라에서 보고돼 왔다. CADA 제안이 이식성 의무와 함께 전환 지원 기간을 규정하려는 것도 이런 현실적인 장벽을 염두에 둔 설계로 보인다.

사유 해지권과 이식성 의무를 법으로 명시하는 일에는 또 다른 법적 긴장이 따라붙는다. 유럽연합의 공공조달 지침(Directive 2014/24/EU)과 유럽연합이 가입한 세계무역기구 정부조달협정은 원칙적으로 자격을 갖춘 외국 공급자를 조달 과정에서 부당하게 차별하지 못하도록 규정한다. 국가 안보와 국방을 이유로 한 예외는 유럽연합 기능조약 제346조에 근거를 두고 있지만, 이 예외는 어디까지나 예외로 설계됐지 원칙으로 설계되지 않았다.

CADA가 SEAL의 상위 단계에서 사실상 비유럽 기업을 조달에서 배제하는 효과를 낳는다면, 그 배제가 안보 예외의 정당한 범위 안에 있는지를 둘러싼 법적 다툼이 뒤따를 가능성이 있다. 이 긴장은 CADA가 유럽의회와 이사회의 심의를 거치는 동안 조문의 표현 하나하나를 두고 계속 다뤄질 사안으로 남아 있다.

이 문제의 무게를 가늠하게 하는 또 다른 숫자가 있다. 팔란티어는 2026년 2분기 실적 발표에서 전년 동기 대비 93퍼센트라는 매출 성장률을 기록했다고 밝혔다. 유럽 각국이 자국의 치안과 국방 영역에서 팔란티어와 거리를 두겠다고 선언하는 동안에도, 유럽의 투자은행과 자산운용사들은 팔란티어 주식을 사들이는 데 수십억 유로를 투입해 왔다고 독일 매체 넷츠폴리티크는 보도했다. 공공조달의 문에서는 밀어내면서 금융시장의 창으로는 자본을 들여보내는 이 모순은, 법 조항 하나로 해결되지 않는다.

이식성 의무는 방향을 가리지 않는 도구라는 점도 놓치지 말아야 한다. 데이터를 쉽게 옮길 수 있게 만드는 규정은 유럽 기업으로 옮겨 가는 길만 여는 것이 아니라, 다른 미국 기업으로 옮겨 가는 길도 함께 연다. 사유 해지권과 이식성 의무 자체는 특정 국적의 기업을 우대하는 장치가 아니라, 공공기관의 협상력을 전반적으로 높이는 장치에 가깝다. 그 협상력이 실제로 유럽 기업을 선택하는 결과로 이어지려면, 결국 SEAL 체계가 규정하는 국적과 지배

구조 요건이 함께 작동해야 한다.

주권을 지키겠다는 선언과, 그 선언을 뒷받침할 유럽산 대체 소프트웨어의 실제 공급 능력 사이에는 여전히 간극이 남아 있다. CADA의 해지권과 이식성 의무는 이 간극을 메우기 위한 제도적 첫걸음이다. 그 첫걸음이 실제 조달 현장에서 작동하는지는 유럽의회의 심의 결과와 그 이후의 시행 과정에서 드러날 것이다.

근거자료

1. 영국 하원 과학기술위원회, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', House of Commons, 2026년.

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

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

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, 2026년.

5. Jan Ebert(얀 에벌), 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026년.

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

제5장. 유로스택과 독자 대안 생태계 구축의 도전

5.1. 프란체스카 브리아의 '유로스택(EuroStack)' 구상과 3,000억 유로의 투자 장벽

프란체스카 브리아는 이탈리아 출신의 경제학자로, 유럽연합 집행위원회 자문으로 활동해 왔다. 그는 바르셀로나 시청에서 디지털 혁신 위원을 지내며, 시민이 만든 데이터를 민간 기업이 아닌 도시 스스로 관리하게 하는 정책을 이끈 경력을 갖고 있다. 이 경력은 그가 훗날 유럽 차원의 디지털 정책을 설계하면서 되풀이해서 인용하는 준거점이 된다. 브리아는 여러 발언과 글에서, 공공 인프라를 미국의 민간 기술 기업에 넘기는 흐름이 민주주의의 기반을 흔들 수 있다는 우려를 밝혀 왔다.

이 책의 앞선 장들이 다룬 사건들, 곧 프랑스 DGSI의 팔란티어 이탈이나 앤트로픽의 접근 차단 사건은 이 우려가 추상적인 걱정에 그치지 않는다는 것을 보여주는 구체적인 사례로 볼 수 있다. 브리아가 유로스택을 설계하며 반복해서 강조하는 지점도, 계약서의 조항이 아니라 인프라 자체를 소유하고 통제하는 주체가 누구인가라는 질문이다.

탐사보도매체 폴로우더머니가 보도한 바에 따르면, 브리아는 '권위주의 스택(The Authoritarian Stack)'이라는 별도 연구를 통해 유럽의 투자은행과 자산운용사가 팔란티어 같은 미국 기업에 대규모 자본을 대는 흐름을 짚었다. 유럽의 연기금과 은행이 자국의 공공 인프라를 잠식하는 기업에 오히려 자금을 대주는 모순을 지적한 것이다. 이 지적은 이 절 뒤에서 다룰 유럽 내부 투자 자본의 흐름 문제와 맞닿아 있다.

이 우려를 구체적인 설계도로 옮긴 결과물이 유로스택 보고서다. 정식 제목은 「EuroStack - A European Alternative for Digital Sovereignty」이며, 브리아와 파울 팀머스, 파우스토 게르노네가 함께 썼다. 독일의 민간 재단 베르텔스만 슈티프퉁이 2025년 2월 13일 이 보고서를 펴냈다. 베르텔스만 슈티프퉁은 독일의 대형 미디어 그룹 베르텔스만이 세운 비영리 재단으로, 오랫동안 유럽의 사회·경제 정책 연구를 후원해 왔다.

이 재단이 유로스택 보고서를 펴냈다는 것은, 이 보고서가 유럽연합의 공식 문서가 아니라 정책 연구 재단이 후원한 독립적인 제안서라는 뜻이다. 이 사실부터 짚어 두어야 한다. 유로스택은 유럽연합이 채택한 법이나 정책이 아니다. 민간 재단이 발간한 정책 제안서이며, 저자들이 유럽연합과 회원국 정부에 이런 방향으로 움직일 것을 촉구하는 문서다. 이 장에서 다루는 수치와 설계는 모두 이 제안서 안에 담긴 내용이며, 실제로

집행되고 있는 예산이나 이미 제정된 규범과는 구분해서 읽어야 한다.

제4장에서 다룬 클라우드·AI 개발법(CADA)과 이 보고서는 서로 다른 층위에 있다. CADA는 유럽연합 집행위원회가 유럽의회와 이사회에 제출한 규정 제안으로, 정식 입법 절차를 밟고 있다. 유로스택은 그 절차 밖에 있는 민간 재단의 정책 보고서다. CADA가 데이터센터를 유럽 안에 짓는 문제와 그 운영 기업의 국적을 가리는 문제를 다룬다면, 유로스택은 그보다 훨씬 넓은 범위인 반도체부터 인공지능까지 일곱 개 층 전체를 자립화하자는 구상이다.

두 문서는 유럽의 기술 자립이라는 같은 목표를 공유하지만, 하나는 입법 절차를 밟는 규정 제안이고 다른 하나는 그 절차 밖에서 방향을 제시하는 정책 제안서라는 점에서 법적 무게가 다르다.

브리아는 유로스택 구상을 설명하면서 유럽 단일 통화인 유로화의 도입에 견주는 표현을 써 왔다. 회원국마다 다른 통화를 쓰던 시절 유럽이 화폐 장벽을 허물고 공동의 금융 질서를 세웠던 것처럼, 디지털 인프라 영역에서도 회원국별로 흩어진 역량을 하나로 모아야 한다는 것이 이 비유의 취지다. 유로화가 도입되기까지 여러 해에 걸친 협상과 조약 개정이 필요했다는 점을 떠올리면, 이 비유는 유로스택이 목표로 하는 통합의 규모가 크다는 것을 강조하려는 의도로 읽을 수 있다.

보고서는 유럽의 디지털 기반을 일곱 개 층으로 나눈다. 가장 아래에는 반도체와 배터리를 만드는 데 필요한 원자재, 그리고 데이터센터를 돌리는 데 필요한 에너지와 물이 놓인다. 그 위에 반도체 칩을 만드는 층, 광대역 통신망을 까는 층, 센서와 사물인터넷 기기를 만드는 층, 클라우드 인프라를 운영하는 층이 차례로 쌓인다. 맨 위에는 소프트웨어 층과 데이터·인공지능 층이 자리한다. 보고서는 이 일곱 층 가운데 어느 하나라도 유럽 바깥의 기업이 쥐고 있으면, 그 위에 쌓은 나머지 층의 자립은 온전할 수 없다고 주장한다.

반도체를 자국에서 만들어도 그 반도체가 들어가는 서버를 미국 회사가 소유한 데이터센터에서만 돌린다면, 자립은 절반짜리에 그친다는 논리다.

이 일곱 층 구조를 집을 짓는 순서에 빗대어 보면 이해하기 쉽다. 아무리 튼튼한 자재로 벽을 세워도, 그 위에 얹을 지붕을 다른 사람의 설계도대로 사야 한다면 집 전체의 안전은 지붕을

파는 사람의 손에 달리게 된다. 유로스택 보고서가 말하는 자립도 마찬가지다. 반도체와 통신망, 클라우드까지는 유럽 기업이 만들었더라도, 그 위에서 돌아가는 인공지능 모델과 데이터 관리 소프트웨어를 미국 기업의 제품에 의존한다면, 아래 여섯 개 층에서 이룬 성과는 맨 위층 하나 때문에 흔들릴 수 있다는 것이 보고서의 논지다.

보고서는 이 일곱 층을 결합해 시민에게 직접 제공할 다섯 가지 공동 서비스도 함께 제안한다. 유럽 안에서 연산을 처리하는 주권 클라우드 서비스, 시민 신원을 확인하는 디지털 신분증 지갑, 은행 수수료 없이 결제할 수 있는 디지털 유로 지불 체계, 회원국 사이에 데이터를 안전하게 주고받는 연합 데이터 스페이스, 그리고 유럽이 직접 설계하고 운영하는 인공지능 엔진이다. 다섯 가지 모두 지금은 미국이나 다른 역외 기업의 서비스에 의존하고 있는 영역이며, 보고서는 이 의존을 걷어내는 것이 유로스택 구상의 실질적인 목표라고 설명한다.

다섯 가지 서비스 가운데 시민의 일상과 가장 가까운 것은 디지털 유로 지불 체계다. 지금 유럽에서 카드로 결제하면 그 거래 정보는 대개 미국계 카드 회사의 결제망을 거친다. 상점이 카드 결제를 받을 때마다 내는 수수료 가운데 상당 부분이 이 결제망을 소유한 회사로 흘러간다. 보고서가 제안하는 디지털 유로 체계는 이 결제망 자체를 유럽 중앙은행 체계 안에 두어, 거래 정보가 역외로 나가지 않게 하고 수수료 구조도 바꾸려는 구상이다. 디지털 신분증 지갑도 비슷한 문제의식에서 나왔다.

시민이 온라인에서 신원을 증명할 때 특정 빅테크의 로그인 체계를 거치는 지금의 관행 대신, 국가가 직접 관리하는 신원 확인 수단을 갖추자는 것이다. 이 다섯 가지 서비스 가운데 디지털 신분증 지갑만큼은 유로스택 보고서가 처음 제안한 개념이 아니라는 점도 짚어 둘 만하다. 유럽연합은 이미 2024년 유럽 디지털 신원 규정, 이른바 eIDAS 2.0을 채택해, 회원국이 시민에게 유럽연합 디지털 신원 지갑을 제공하도록 의무화했다. 이 규정은 유로스택 보고서와 별개로 이미 제정되어 시행에 들어간 법이다.

유로스택 보고서는 이 기존 제도를 폐기하고 새로 만들자는 것이 아니라, 이미 진행 중인 이 흐름을 일곱 개 층 구조 안에 포함시켜 다른 층과 유기적으로 연결하자고 제안하는 쪽에 가깝다. 나머지 세 가지 서비스는 정부와 기업이 마주하는 층위에 가깝다. 주권 클라우드 서비스는 제4장에서 다룬 CADA의 주권 보증 수준 체계와 지향점이 겹친다.

아마존웹서비스나 마이크로소프트가 유럽 고객을 겨냥해 내놓은 이른바 주권형 클라우드 상품이 제4장에서 살펴본 것처럼 지배 지분까지 유럽에 넘기지는 않는다는 한계를 안고 있었던 것과 달리, 유로스택이 말하는 주권 클라우드 서비스는 소유권 자체가 유럽에 있는 클라우드를 가리킨다. 연합 데이터 스페이스는 회원국 정부와 기업이 데이터를 주고받을 때 미국 클라우드를 거치지 않도록 하는 통로다. 이 구상은 제4장에서 다룬 CADA보다 앞서, 2019년 프랑스와 독일이 시작한 가이아엑스(Gaia-X) 프로젝트와도 맥이 닿아 있다.

가이아엑스가 법적 구속력이 없는 자발적 표준화 시도에 그쳤다는 평가를 받았던 것과 달리, 유로스택 보고서는 이 데이터 공유 체계를 국가 예산이 뒷받침하는 공동 인프라로 격상시키자고 제안한다. 소베린 인공지능 엔진은 지금 유럽의 공공기관과 기업이 미국이나 다른 역외 기업이 만든 거대언어모델에 의존하는 상황을 바꾸려는 목표를 담고 있다.

보고서가 제시하는 투자 규모는 작지 않다. 저자들은 이 일곱 층의 인프라를 새로 세우는 데 대략 10년이 걸린다고 추산했고, 2035년까지 총 3,000억 유로에 이르는 자본이 필요하다고 밝혔다. 여기에 더해 초기 마중물 역할을 할 100억 유로 규모의 별도 기술 기금을 신설하자는 제안도 담았다. 3,000억 유로를 10년으로 나누면 한 해 평균 300억 유로 규모의 투자가 꾸준히 이어져야 한다는 뜻이다. 이 수치는 보고서 저자들의 계산이며, 유럽연합이 공식적으로 채택하거나 배정한 예산이 아니다.

이 액수를 유럽연합이 실제로 움직이고 있는 예산과 나란히 놓아 보면 간극이 드러난다. 정책 연구 기관 CERRE가 2025년 9월 낸 보고서는, 유럽연합이 추진하는 경쟁력 기금 안에서 디지털 주권 관련 항목에 배정된 예산이 550억 유로 수준이라고 밝혔다. 유로스택 보고서가 요구하는 3,000억 유로와 견주면 5분의 1에도 못 미치는 규모다. 경쟁력 기금은 유럽연합이 2028년부터 시작되는 차기 다년도 예산 틀 안에서 디지털과 산업 경쟁력 강화를 위해 편성하려는 예산 항목으로, 아직 회원국과 유럽의회의 최종 승인을 남겨 두고 있다.

이 예산 자체도 확정된 액수가 아니라는 뜻이며, 그 안에서도 디지털 주권에 배정된 몫은 유로스택이 요구하는 액수에 크게 못 미친다. 이 비교가 뜻하는 바는 분명하다. 유로스택은 방향을 제시하는 설계도이지, 그 설계도를 완성할 예산이 이미 확보됐다는 뜻은 아니다.

브리아를 비롯한 유럽의 정책 논의 참여자들은 이 자금 격차를 메울 곳으로 정부 예산이 아닌 민간의 저축을 지목한다. 매체 EU 퍼스펙티브스가 2026년 1월 보도한 바에 따르면, 유럽연합 가계가 은행 계좌에 넣어 둔 예금 총액은 2026년 기준으로 30조 유로를 웃돈다. 세계경제포럼이 2026년 1월 연차총회에서 진행한 토론에서 거론된 수치로는, 이 액수가 유럽연합 전체 국내총생산의 두 배를 넘는다. 문제는 이 돈이 움직이지 않는다는 데 있다.

폴리티코 유럽판이 2026년 6월 4일 다룬 토론에서 언급된 내용에 따르면, 스웨덴처럼 시민의 절반 이상이 주식이나 펀드에 돈을 넣는 나라가 있는 반면, 유럽의 여러 대형 회원국에서는 그 비율이 2퍼센트 안팎에 머문다. 은행에 잠긴 돈은 스타트업으로 흘러가지 못하고, 정작 투자로 나가는 돈의 상당 부분은 미국의 대형 기술주로 향한다고 이 토론은 지적했다.

연금 기금도 비슷한 문제를 안고 있다. 프랑스24가 2026년 6월 방영한 토론에서 짚은 내용에 따르면, 유럽의 연금 기금은 안정성을 우선하는 감독 규정에 묶여 있어 성장 초기 단계의 기술 기업에 자금을 대기가 어렵다. 유럽연합의 보험·연금 감독 체계인 솔벤시 투(Solvency II) 같은 규정은 연금 기금이 갑작스러운 손실을 보지 않도록 안전자산 비중을 일정 수준 이상 유지하게 한다.

이 규정의 취지는 은퇴자의 노후 자금을 지키는 데 있지만, 결과적으로 성장 초기 단계의 기술 기업처럼 위험이 크고 수익도 불확실한 자산에 연금 자금이 흘러가는 길을 좁히는 효과도 함께 낸다. 이 자금 경색은 인재 유출로도 이어진다. 자금을 구하지 못한 유럽의 기술 인력이 미국 실리콘밸리로 옮겨 가는 흐름이 같은 토론에서 언급됐다. 유럽연합 집행위원회가 CADA 제안과 함께 낸 부속 실무 문서 SWD(2026) 502 final은 이 자금 격차를 수치로도 보여준다.

전 세계 벤처캐피털 투자액 가운데 유럽이 차지하는 비중은 5퍼센트에 그치는 반면, 미국은 52퍼센트를 차지한다. 브리아는 2024년 CEPS 강연에서, 유럽에서 태어난 성공적인 스타트업 가운데 상당수가 사업을 키우는 단계에 이르러 외국 자본에 인수돼 유럽 밖으로 나간다고 지적했다.

이런 진단에 따라 브리아는 은행 예금과 연금 자산이 유럽의 기술 기업으로 흘러가도록 유도하는 세제 개편을 요구해 왔다. 저축을 오래 묶어 두는 대신 국내 기술 기업에 넣는

시민에게 세금을 깎아 주거나, 연금 기금이 위험자산에 투자할 수 있는 한도를 넓히는 방식이 거론된다. 이런 제안이 실제 입법으로 이어졌는지는 이 책이 확인한 자료 범위 안에서는 아직 확정되지 않았다. 유로스택 보고서가 요구하는 3,000억 유로 가운데 상당 부분을 정부 예산이 아닌 민간 자본으로 채우려 한다면, 이런 세제 개편이 선행되어야 한다는 것이 보고서의 논리다.

자금이 전혀 움직이지 않는 것은 아니다. 프랑스어권 경제 매체 에코퀵이 2026년 6월 4일 보도한 바에 따르면, 유럽연합은 인공지능 기가팩토리를 짓는 데 200억 유로 규모의 공공 자금을 투입하는 계획을 확정했다. 스페인 총리실은 2026년 7월 1일 발표에서, 자국의 인공지능 기가팩토리를 짓는 데 7억 2,000만 유로의 공공 예산을 투입하는 협정을 승인했다고 밝혔다. 스웨덴계 자산운용사 이큐티가 운용을 맡은 50억 유로 규모의 스케일업 유럽 펀드도 2026년 가을부터 자금 집행을 시작할 예정이라고 매체 스타트업 온라인이 2026년 5월 21일 전했다.

이 펀드는 독일 개발은행 KfW가 조성한 10억 유로 규모의 딥테크 펀드와 함께 움직인다.

이 실제 집행 금액을 모두 더해도 200억에 7억 2,000만, 50억을 합쳐 300억 유로에 못 미친다. 유로스택 보고서가 요구한 3,000억 유로의 10분의 1 수준이다. 유럽연합과 몇몇 회원국이 실제로 지갑을 연 것은 사실이지만, 그 규모는 브리아가 제시한 설계도를 채우기에는 아직 한참 모자란다.

이 숫자들을 나란히 놓아 보면 문제의 성격이 더 뚜렷해진다. 유럽연합 가계가 은행에 쌓아 둔 예금은 30조 유로를 웃돌고, 유로스택 보고서가 요구하는 투자액은 3,000억 유로다. 산술적으로만 보면 이 예금의 1퍼센트만 기술 투자로 옮겨져도 보고서가 요구하는 액수 전체를 채울 수 있다는 뜻이다. 문제는 이 1퍼센트를 움직이게 할 유인과 제도가 아직 갖춰지지 않았다는 데 있다. 돈이 없어서가 아니라, 그 돈을 저축에서 투자로 옮기게 할 세제와 금융 상품, 신뢰가 부족하다는 것이 이 격차의 본질에 가깝다.

이 격차가 좁혀지지 않으면 유로스택이 그리는 일곱 개 층 가운데 상당수는 설계도 단계에 머무를 수밖에 없다. 반도체나 데이터센터처럼 막대한 초기 투자가 필요한 층일수록 이 자금 부족의 영향을 먼저 받는다. 회원국별로 예산을 나누어 편성하는 지금의 방식으로는 3,000억 유로 규모의 사업을 감당하기 어렵다는 지적이 나오는 이유이며, 브리아가 민간

저축과 연금 자산까지 끌어들이려는 것도 이 때문이다.

유럽연합이 2028년부터 시작될 차기 예산 협상에서 디지털 주권 예산을 얼마나 늘릴지가, 유로스택 구상이 설계도에서 실제 사업으로 넘어갈 수 있을지를 가늠하는 다음 시험대가 될 것으로 보인다. 그 협상의 결과가 나오기 전까지, 유로스택은 유럽이 나아가려는 방향을 가리키는 지도이지, 이미 완공된 건물은 아니다.

근거자료

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

2. Johanna Bröer 등, 'Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?', CERRE Issue Paper, 2025년 9월, 17쪽.

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

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

5. POLITICO Europe, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, 2026년 6월 4일, 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, 2026년 6월.

7. European Commission, SWD(2026) 502 final, 유럽연합 관보, 2026년 6월 3일, 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, 2024년.

9. 로익 크라프트, 'Souveraineté numérique : Bruxelles renâcle à imposer des contraintes trop fortes', 에코퀵, 2026년 6월 4일.

10. 스페인 총리실, 'The President calls for public-private partnership to drive forward Spain's artificial intelligence gigafactory', La Moncloa, 2026년 7월 1일.

11. 스타트업 온라인 편집국, '유럽 디지털 주권을 위한 연산력·클라우드·오픈소스·자본에 관한 연구 보도', Startup Online, 2026년 5월 21일.

5.2. 대안 소프트웨어 동맹: 아르카디아(Arcadia)와 오픈 소스 디지털 공공재

지휘통제 시스템, 흔히 C2라 줄여 부르는 소프트웨어는 전장에서 벌어지는 일을 화면에 모아 보여주고 지휘관의 명령을 부대에 전달하는 도구다. 어느 부대가 어디에 있는지, 어떤 표적이 발견됐는지, 어느 부대에 어떤 명령이 내려갔는지를 실시간으로 정리해 보여준다. 제3장에서 다룬 메이븐 스마트 시스템이 나토 동맹 차원에서 이 역할을 맡고 있다면, 아르카디아는 프랑스가 같은 역할을 자국의 소프트웨어로 대체하려는 시도다.

프랑스는 팔란티어의 메이븐 스마트 시스템을 대신할 자국 주도의 군사용 인공지능 지휘통제 체계를 개발하고 있다. 이름은 아르카디아다. 방산 매체 아르메닷컴과 이코노미 마탱이 2026년 7월 9일 함께 전한 바에 따르면, 아르카디아는 탈레스와 에어버스, 사프란, 그리고 프랑스의 대형 언어모델 개발사 미스트랄 AI가 컨소시엄을 이뤄 만들고 있는 전장 지휘 소프트웨어다. 여기에 코맨드 AI와 임팩트 같은 전술 소프트웨어 스타트업도 결합했다.

미스트랄 AI는 2023년 파리에서 설립된 대형 언어모델 개발사로, 유럽에서 나온 인공지능 기업 가운데 가장 앞선 자리를 차지하고 있다는 평가를 받는다. 이 회사가 군사용 컨소시엄에 참여했다는 사실은, 유럽의 민간 인공지능 산업이 국방 영역과도 결합하고 있다는 것을 보여준다.

아르카디아는 아무것도 없는 데서 출발한 사업이 아니다. 같은 보도에 따르면, 프랑스는 이전에도 탈레스와 소프라 스테리아가 함께 진행한 전투 지휘소 시스템 SIA C2를 여러 해 동안 추진했지만, 기술 불합치 문제로 사업이 취소된 경험이 있다. 아르카디아 컨소시엄은 이 실패를 교훈 삼아 시스템을 처음부터 모듈식으로 설계했다. 개방형 인터페이스(API)를 적용해 여러 회사가 만든 소프트웨어 조각이 서로 결합할 수 있도록 하고, 동맹군 사이의 무선 통신을 지원하는 나토의 연합 임무 네트워크(FMN) 표준도 충족시켰다.

FMN은 나토 회원국의 서로 다른 지휘통제 시스템이 연합 작전에서 정보를 주고받을 수 있도록 정해 둔 공통 규격이다. 한 나라의 부대가 자국의 시스템으로 확인한 표적 정보를, FMN 표준을 따르는 다른 나라의 시스템에서도 같은 형식으로 읽을 수 있게 하는 것이 이 표준의 목적이다. 아르카디아가 이 표준을 충족시켰다는 것은, 프랑스가 독자적인

소프트웨어를 쓰면서도 동맹군과의 정보 공유 능력을 포기하지 않았다는 뜻이다. 국가의 독자 설계권과 동맹군과의 상호 운용성을 동시에 만족시키려는 설계다.

모듈식 설계란 커다란 완제품 하나를 통째로 사는 대신, 표준화된 조각을 여러 회사에서 사다가 조립하는 방식이다. 어느 한 조각을 만든 회사가 문을 닫거나 계약을 끊어도, 같은 규격에 맞는 다른 회사의 조각으로 바꿔 끼우면 전체 시스템은 계속 돌아간다. 이전의 SIA C2 사업이 특정 공급업체의 폐쇄적인 설계에 발목을 잡혔던 것과 달리, 아르카디아는 이 모듈식 구조 덕분에 특정 기업 하나의 사정에 시스템 전체가 좌우되는 위험을 줄이려 한다.

CWIX는 연합군 상호 운용성 훈련을 뜻하는 나토의 정례 행사로, 회원국이 개발한 무기 체계와 통신 장비가 실제로 서로 연동되는지를 해마다 점검하는 자리다. 새로 개발된 지휘통제 소프트웨어가 동맹군의 다른 장비와 실제로 통신할 수 있는지를 이 훈련에서 시험하는 것이 관례로 자리 잡았다. 아르카디아는 2026년 6월 폴란드 비드고슈치에서 열린 이 훈련에서 처음 시험 운용됐다. 국방 전문 매체 디펜스뉴스가 2026년 6월 5일 전한 바에 따르면, 이 훈련은 아르카디아가 실전 환경에서 데이터를 처리하는 능력을 검증하는 자리였다.

완성된 시스템을 실전에 전면 배치한 것이 아니라, 개발 중인 시스템을 나토 표준 아래에서 시험한 단계라는 뜻이다. 같은 보도에 따르면, 프랑스 육군 차장 패트릭 쥐스텔 장군은 이 훈련에서 검증 없이 외국의 소프트웨어를 받아들이는 태도는 국가 주권을 스스로 내주는 일이라고 말했고, 아르카디아가 미국의 군사 기술 우위에 대한 프랑스의 응답이라고 설명했다.

아르카디아와 메이븐의 개발 방식에는 뚜렷한 차이가 있다. 팔란티어는 메이븐 스마트 시스템을 자사가 소유한 소프트웨어로 개발해 나토에 공급하는 단일 공급자 방식을 택했다. 아르카디아는 반대로 탈레스와 에어버스, 사프란, 미스트랄 AI, 그리고 여러 스타트업이 각자의 전문 영역을 모듈 형태로 만들어 결합하는 컨소시엄 방식을 택했다. 어느 한 회사가 시스템 전체를 좌우하지 못하게 하려는 설계다. 이 방식은 개발 속도를 늦출 수 있다는 단점이 있지만, 특정 기업 하나에 안보 인프라 전체를 의존하는 위험을 줄인다는 장점도 있다.

이 흐름은 프랑스에 국한되지 않는다. 매체 더넥스트웹이 2026년 7월 18일 전한 바에 따르면, 프랑스와 독일 정부는 팔란티어의 군사용 인공지능 소프트웨어에 맞설 유럽 차원의 경쟁 체계를 함께 만들겠다고 공동으로 다짐했다. 이 다짐이 구체적인 공동 개발 계획으로 이어졌는지, 아니면 각국이 아르카디아처럼 독자적인 사업을 계속 추진하는 데 그쳤는지는 이 책이 확인한 자료로는 분명하지 않다. 컨설팅 업체 패스파운더스그룹이 2026년 4월 정리한 목록에 따르면, 유럽 안에서 팔란티어의 대안으로 거론되는 기업은 아르카디아 컨소시엄 참여사 외에도 여러 곳이 더 있다.

하나의 승자가 정해지기보다 여러 기업이 각자의 영역에서 경쟁하는 구도가 형성되고 있다는 뜻이다.

아르카디아는 지금까지 프랑스가 주도하는 사업이며, 컨소시엄에 참여한 기업도 대부분 프랑스 회사다. CWIX 훈련은 나토 회원국이 함께 참여하는 다국적 행사였지만, 아르카디아 자체가 나토 전체의 공식 표준으로 채택된 것은 아니다. 프랑스 바깥의 다른 회원국이 이 시스템을 실제로 도입할지, 아니면 각국이 저마다 자국에서 개발한 별도 시스템을 쓸지는 이 책이 확인한 자료 범위 안에서는 아직 정해지지 않았다. 만약 유럽 각국이 서로 다른 지휘통제 시스템을 따로 개발한다면, 이번에는 유럽 국가들 사이의 상호 운용성이 새로운 과제로 떠오를 수 있다.

이 컨소시엄에서 사프란이 맡은 역할은 별도로 살펴볼 만하다. 프랑스 경제 매체 레상시엘드 레코가 2026년 6월 8일 전한 바에 따르면, 항공기 엔진 제작사로 출발한 사프란은 2022년부터 정보 분석 관련 기업을 잇달아 인수했다. 2022년 7월에는 재밍 환경에서도 정확한 위치 신호를 제공하는 오롤리아를 1억 100만 달러에 인수했고, 2024년에는 위성 영상 분석 기업 프레리전스를 2억 2,000만 유로에 흡수해 사프란.AI 부서를 새로 출범시켰다. 2026년 2월에는 지하 공간 항재밍 기술을 가진 신토니를, 2026년 5월에는 레이더 영상 분석 기업 케이로스의 국방 부문을 추가로 인수했다.

같은 보도에 따르면 사프란.AI 부서는 300명의 엔지니어를 두고 있으며, 2025년 매출이 전년 대비 65퍼센트 늘었고 2026년에는 90퍼센트 성장을 내다보고 있다고 한다. 이 부서가 개발한 표적 인식 엔진 ACE는 싱가포르와 캐나다, 인도의 파트너와 공동 개발 협정을 맺는 데도 쓰이고 있다고 이 매체는 전했다. 이 협력국 명단이 뜻하는 바도 짚어 둘 만하다.

싱가포르와 인도는 미국이 주도하는 정보 공유 동맹인 파이브 아이즈에 속하지 않으면서도 서방과 안보 협력을 맺어 온 나라들이다.

사프란이 이런 나라들과도 손잡는 것은, 미국 중심의 정보 동맹 바깥에서 별도의 정보 협력망을 넓히려는 시도로 읽을 수 있다. 항공기 엔진을 만들던 회사가 몇 해 사이 정보 분석 기업을 연쇄적으로 사들여 인공지능 기업으로 몸집을 바꾼 이 사례는, 유럽의 방산 대기업들이 소프트웨어와 데이터 역량을 자체 개발하는 대신 인수를 통해 빠르게 확보하는 흐름을 보여주는 사례이기도 하다.

군사 영역 바깥에서는 오픈 소스 소프트웨어를 중심으로 한 움직임이 진행되고 있다. 유럽연합 집행위원회가 2026년 6월 3일 낸 관보 문서 COM(2026) 503 final은, 유럽연합 회원국들이 미국계 소프트웨어 구독료로 지불하는 비용이 연간 2,640억 유로에 이른다고 추산했다. 같은 문서는 이 비용을 줄이기 위해 공공 예산으로 만든 소프트웨어의 소스코드를 시민에게 무상으로 공개하자는 원칙, 이른바 공공 예산·공공 코드 원칙을 담은 오픈 소스 전략을 제시했다.

이 비용이 반복되는 이유는 소프트웨어 산업 특유의 잠금 효과에 있다. 한 관청이 특정 회사의 사무용 소프트웨어로 문서를 만들고 저장하기 시작하면, 몇 해가 지난 뒤 다른 회사의 제품으로 옮기려 해도 문서 형식과 업무 절차가 이미 그 회사의 방식에 맞춰져 있어 전환 비용이 눈덩이처럼 불어난다. 매년 내는 구독료보다 이 전환 비용에 대한 부담이 더 커서, 관청은 계약을 갱신하는 쪽을 택하게 된다. 오픈 소스 전략이 겨냥하는 것은 이 잠금 구조 자체다.

소스코드를 공개해 여러 회사가 같은 코드 기반 위에서 경쟁하게 하면, 한 공급업체에 발이 묶이는 상황을 막을 수 있다는 논리다.

이 원칙에 따라 프랑스와 독일, 이탈리아, 네덜란드 정부는 2025년 10월 디지털 커먼즈 EDIC이라는 이름의 유럽 디지털 인프라 컨소시엄을 결성했다. EDIC은 유럽 디지털 인프라 컨소시엄의 줄임말로, 여러 회원국이 공동 사업을 벌일 때 쓰는 법적 조직 형태다. 각 정부가 개별적으로 계약을 맺는 대신, 이 조직 하나가 참여국을 대표해 예산을 모으고 사업을 관리한다. 이 컨소시엄의 중심에는 독일 연방 내무부가 마이크로소프트 365의 대안으로 개발을 승인한 사무 협업 소프트웨어 오펜데스크(openDesk)가 있다.

오펜데스크는 파일 저장 도구 넥스트클라우드, 메일 서버 오펜익스체인지, 콘텐츠 관리 도구 드루팔, 분산형 메신저 매트릭스를 하나로 묶은 소프트웨어 모음이다. 각 지방 정부가 소스코드를 따로 고쳐 쓰는 대신 오펜코드라는 공유 저장소를 통해 소스코드를 함께 관리한다. 이 오픈 소스 전략은 원스온리라 불리는 행정 원칙과도 함께 추진된다고 독일 조달 전문 매체 코시넥스 블로그가 전한다. 원스온리는 시민이나 기업이 한 번 제출한 서류나 정보를 여러 관청에 중복해서 다시 내지 않아도 되도록, 관청들이 이미 제출된 정보를 서로 공유하게 하는 원칙이다.

소스코드를 공유하는 오펜코드와, 행정 정보를 공유하는 원스온리는 서로 다른 대상을 다루지만, 중복을 줄이고 자원을 공유한다는 같은 발상에서 나왔다. 프랑스의 협업 소프트웨어 라 스위트와 독일의 오펜데스크, 네덜란드의 메인뷔로는 서로 다른 세 나라의 소프트웨어가 외국 클라우드를 거치지 않고 문서를 주고받을 수 있다는 것을 실제로 시연해 보였다고 관련 보도는 전한다. 이 시연이 뜻하는 바는 작지 않다. 지금까지는 서로 다른 나라의 공무원이 문서를 주고받으려면 결국 같은 미국계 클라우드 계정으로 모이는 경우가 많았다.

세 나라가 각자 다른 소프트웨어를 쓰면서도 서로 연동할 수 있다는 것을 보였다는 것은, 유럽 국가들이 하나의 소프트웨어로 통일하지 않고도 상호 운용성을 확보할 길이 있다는 뜻이다.

이 오픈 소스 전략은 제4장에서 다룬 CADA의 주권 보증 수준 체계와도 맞물릴 것으로 보인다. 오펜데스크나 라 스위트 같은 일반 행정용 소프트웨어는 SEAL 체계에서 상대적으로 민감도가 낮은 하위 단계에 해당할 가능성이 크고, 아르카디아처럼 국방과 직결된 소프트웨어는 상위 단계의 엄격한 요건을 적용받을 가능성이 크다. 다만 오픈 소스 소프트웨어와 SEAL 등급 체계가 실제로 어떻게 맞물릴지는 CADA가 최종 조문을 확정하는 과정에서 구체화될 사안이다.

지방 정부 단위의 사례도 있다. 유럽연합 집행위원회의 인터오퍼러블 유럽 포털이 정리한 자료에 따르면, 독일 북부 슐레스비히홀슈타인주는 2020년부터 공무원 컴퓨터 2만 5,000대에서 마이크로소프트 운영체제와 아웃룩을 걷어내고 리브레오피스로 전환하는 작업을 진행했다. 주정부가 2025년 12월 4일 낸 보도자료에 따르면, 이 전환으로 주정부는

연간 1,500만 유로의 소프트웨어 라이선스 비용을 절감했다.

스위스는 법 제정으로 더 나아갔다. 스위스 언론 왓슨이 2024년 12월 4일 보도한 바에 따르면, 스위스는 2024년 전자정부 전자수단법(EMBAG)을 통과시켜, 공공 예산으로 만든 모든 소프트웨어의 소스코드를 원칙적으로 오픈 소스로 공개하도록 의무화했다. 같은 법에 따라 스위스 연방군 참모부 사이버사령부는 자체 개발한 보안 분석 소프트웨어 룸(Loom)을 민간에 무상으로 공개했다. 군이 자체 개발한 소프트웨어를 오픈 소스로 내놓는 사례는 흔치 않다는 점에서, 이 결정은 스위스가 자국의 기술 자립을 어디까지 밀어붙이려 하는지를 보여준다.

이 흐름은 제1장에서 살펴본 프랑스 국내보안총국(DGSI)의 아르곤OS 전환, 독일 헌법수호청의 이탈과도 같은 줄기 위에 있다. 제1장이 다룬 것은 기존에 팔란티어가 맡고 있던 업무를 다른 공급업체의 제품으로 옮기는 국내 정보기관의 결정이었다면, 이 절에서 다룬 아르카디아와 오펜데스크는 그 대체재를 유럽 스스로 만들어 내려는 개발 사업이라는 차이가 있다. 조달처를 바꾸는 결정과, 바꿀 수 있는 제품 자체를 만드는 작업은 서로 다른 단계의 과제다.

아르카디아와 오펜데스크, EMBAG은 서로 다른 층위에서 움직이는 사업이다. 아르카디아는 군사 지휘통제 소프트웨어를, 오펜데스크는 공공 행정의 사무용 소프트웨어를, EMBAG은 소스코드 공개 의무를 법으로 정하는 일을 각각 다룬다. 이 셋이 공유하는 지점은 하나다. 외국 기업의 상업 제품을 빌려 쓰는 대신, 유럽 안에서 소스코드를 소유하고 고칠 수 있는 소프트웨어를 만들겠다는 판단이다.

이 판단이 얼마나 널리 퍼질지는 아직 지켜봐야 한다. 슐레스비히홀슈타인주나 스위스 연방군처럼 눈에 띄는 성과를 낸 사례가 있는 한편, 유럽연합 전체 회원국이 같은 속도로 오픈 소스 전환에 나서고 있는 것은 아니다. 마이크로소프트나 구글의 소프트웨어에 이미 깊이 얽혀 있는 관청일수록 전환에 드는 초기 비용과 직원 재교육 부담이 크고, 이 부담을 감수할 정치적 의지가 모든 회원국에서 같은 정도로 형성돼 있지는 않다. 아르카디아와 오펜데스크가 보여준 것은 가능성이지, 유럽 전역에 걸친 완결된 전환이 아니다.

근거자료

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

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

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

4. L'Essentiel de l'Éco 편집국, 'Comment Safran devient un géant du renseignement par IA', L'Essentiel de l'Éco, 2026년 6월 8일.

5. European Commission, COM(2026) 503 final, 유럽연합 관보, 2026년 6월 3일, https://ec.europa.eu/newsroom/dae/redirection/document/129100

6. Digital Independence Editorial, 'Digital Sovereignty in Europe', Digital Independence, 2026년 2월 16일.

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

8. 슐레스비히홀슈타인주 정부, 보도자료, 2025년 12월 4일.

9. Watson 편집국, 'Schweizer Armee setzt auf europäische Software statt Microsoft', Watson, 2024년 12월 4일.

10. TNW 편집국, 'France and Germany pledge to build a European rival to Palantir's military AI software', The Next Web, 2026년 7월 18일.

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

12. Wolf Witte, 'Vergabebeschleunigungsgesetz und digitale Souveränität 2026', cosinex Blog, 2026년 5월 21일.

5.3. 조세 회피 다국적 기업에 맞서는 경제 주권: CICTAR 보고서와 공공 재정 보호

유럽 각국 정부는 팔란티어와 같은 미국 기업에 해마다 상당한 조달 예산을 지불하고 있다. 이 지출이 유럽 사회에 세금으로 얼마나 되돌아오는가를 따진 보고서가 2026년 8월 5일 나왔다. 국제기업조세책임성연구소(CICTAR)는 다국적 기업의 조세 회피 구조를 추적해 온 연구 조직으로, 팔란티어 이전에도 여러 다국적 기업의 조세 관행을 분석한 보고서를 낸 바 있다. 이번에는 그 대상을 팔란티어로 좁혔다.

유럽공공서비스노조연맹(EPSU)의 지원을 받아 작성한 이 보고서는, 팔란티어의 조세 구조를 분석해 이 회사가 공공 계약으로 얻은 이익에 비해 매우 적은 세금만 내고 있다고 주장했다. 이 내용은 탐사보도매체 폴로우더머니가 2026년 8월 5일 기사로 정리해 보도했다. EPSU는 공공 부문 노동자를 대표하는 유럽 단위 노동조합 연맹이다. 팔란티어를 비롯한 민간 기업이 공공 조달을 늘리는 흐름은 공공 부문 일자리와 예산에 직접 영향을 미치는 사안이므로, EPSU가 이 조사에 자금을 댄 것은 이해관계가 있는 주체의 지원이라는 점을 밝혀 둘 필요가 있다.

이 사실이 보고서의 분석 내용을 자동으로 무효화하지는 않지만, 독자가 이 보고서를 읽을 때 참고할 만한 배경이다.

이 보고서가 독일 사례를 다루게 된 배경에는 실제 경찰 조달 계약이 있다. 독일 매체 랩아넷 저머니가 전한 바에 따르면, 헤센주를 비롯한 몇몇 독일 주 경찰은 팔란티어의 소프트웨어를 이용해 잠재적 위협 인물, 독일어로 게패어더로 불리는 대상을 추적하고 분석하는 작업을 해 왔다. 이런 계약이 여러 주에서 누적되면서, CICTAR가 추산한 독일 내 세원 손실 규모의 배경이 됐다는 것이 이 보도의 설명이다.

실효세율이란 기업이 실제로 낸 세금을 세전 이익으로 나눈 값이다. 법에 정해진 세율이 아무리 높아도, 각종 공제와 회계 기법을 거쳐 실제로 내는 세금이 줄어들면 실효세율은 그만큼 낮아진다. CICTAR 보고서가 문제 삼는 것은 팔란티어가 법을 어겼다는 것이 아니라, 합법적인 회계 기법을 겹겹이 동원해 이 실효세율을 낮췄다는 점이다. 세법을 위반하는 탈세와, 세법이 허용하는 절차 안에서 세금을 줄이는 조세 회피는 법적으로 다른 범주에 속한다. 이 보고서가 고발하는 것은 후자다. 이런 구분은 이 문제를 다루는 방식에도

영향을 준다.

탈세는 수사와 처벌의 대상이지만, 조세 회피는 개별 기업을 처벌해서 막을 수 있는 문제가 아니다. 세법 자체를 고치거나, 국가 사이의 조세 협정을 다시 짜거나, 조달 계약의 조건을 바꾸는 식의 제도적 대응이 필요하다는 뜻이다. 이 장 뒤에서 살펴볼 BEFIT 제안이나 조달 규격서 개정 요구가 바로 이런 제도적 대응에 해당한다.

CICTAR 보고서는 팔란티어의 2025년 글로벌 법인세 실효세율이 1.4퍼센트에 그쳤다고 주장한다. 보고서에 따르면 팔란티어는 2025년 한 해 동안 세전 이익으로 약 16억 6,000만 달러를 벌어들였지만, 전 세계에 납부한 법인세는 2,270만 달러에 그쳤다. 이 수치는 CICTAR와 폴로우더머니의 분석에 의한 것이며, 이 책은 팔란티어의 원본 재무제표를 별도로 검증하지 못했다. 다만 이 주장이 짚는 문제 자체는 살펴볼 필요가 있다.

경제협력개발기구가 주도하고 140여 개국이 참여한 이 합의는 필라 투(Pillar Two)라 불리며, 2021년 큰 틀에서 합의된 뒤 참여국별로 순차적으로 국내법에 반영되고 있다. 다국적 기업이 어느 나라에서 사업하든 최소 15퍼센트의 법인세를 물리는 것이 이 합의의 목표다. CICTAR 보고서가 제시한 1.4퍼센트라는 수치가 사실이라면, 이는 이 국제 합의의 취지에서 크게 벗어난 결과다.

미국 조세 정책 연구기관 ITEP가 2026년 3월 22일 낸 별도 보고서는, 팔란티어가 트럼프 행정부 시기 제정된 세제 혜택법에 따른 연구개발비 즉시 공제를 활용해 미국 내 연방 법인세를 사실상 내지 않고 있다고 분석했다.

CICTAR 보고서는 팔란티어가 쓰는 회계 기법도 소개한다. 다국적 기업의 본사와 해외 지사 사이에는 흔히 이전가격이라는 것이 오간다. 지사가 본사에 기술 사용료나 서비스 수수료 명목으로 돈을 보내는 거래다. 이 금액을 얼마로 잡느냐에 따라 지사의 장부상 이익이 크게 달라진다. 지사가 본사에 많은 돈을 보내면 지사의 이익은 줄어들고, 그만큼 지사가 소재한 나라에 낼 법인세도 줄어든다. 보고서에 따르면, 유럽 각국의 팔란티어 자회사는 계약에서 발생한 수익을 미국 본사로 송금하고, 그 대가로 미국 본사로부터 적은 액수의 서비스 수수료만 받는 구조로 회계 장부를 짠다.

이 구조에서는 유럽 자회사의 장부상 이익이 실제 영업 규모보다 낮게 잡힌다. 스페인에서는 다른 방식이 쓰였다고 보고서는 전한다. 스페인 자회사가 공공 조달로 벌어들인 이익의 70퍼센트를 기술 사용료 명목으로 미국 본사에 송금해, 과세 대상이 되는 스페인 지사의 이익을 크게 줄였다는 것이다. 여기에 더해 직원에게 현금 대신 자사 주식을 지급하는 주식 보상 제도도, 세법상 비용으로 처리되어 과세 소득을 줄이는 데 쓰인다고 보고서는 지적한다. 회사가 직원에게 주식을 나눠 주면, 그 주식의 가치만큼을 인건비로 회계 장부에 반영할 수 있다.

인건비는 세법상 비용으로 인정되므로, 이 비용이 커질수록 과세 대상이 되는 이익은 줄어든다. 현금으로 월급을 주는 대신 주식으로 지급하는 관행이 널리 퍼진 기술 업계에서 이 방식은 합법적인 절세 수단으로 흔히 쓰인다.

보고서가 제시한 나라별 수치도 있다. CICTAR는 이런 회계 구조로 인해 독일에서 발생한 2024년 세원 손실이 160만 유로에 이른다고 추산했으며, 같은 해 팔란티어 독일 자회사가 실제로 낸 법인세는 64만 유로에 그쳤다고 밝혔다. 스페인에서는 팔란티어가 국가 치안 관련 기관과 1,650만 유로 규모의 계약을 맺었지만, 실제로 낸 법인세는 14만 7,000유로에 불과했다고 보고서는 전한다. 이 수치들은 모두 CICTAR가 분석해 제시한 것이며, 각국 정부의 공식 발표 자료는 아니다.

영국에서는 별도의 사례가 확인된다. 매체 노바라 미디어가 2026년 6월 4일 보도한 바에 따르면, 영국 국민보건서비스(NHS)는 팔란티어와 3억 3,000만 파운드 규모의 통합 데이터 플랫폼 계약을 맺었다. 이 계약은 연방 데이터 플랫폼이라는 이름으로 불리며, 잉글랜드 전역의 병원과 진료 기록을 하나의 시스템으로 통합하려는 사업이다. 팔란티어가 이 사업의 우선협상대상자로 선정된 것은 2023년이며, 환자의 민감한 의료 정보를 다루는 계약이라는 점에서 선정 당시부터 영국 의료계와 정치권에서 논란이 일었다.

같은 보도에 따르면 팔란티어 영국 자회사가 2024년 영국 세무당국에 낸 법인세는 200만 파운드에 그쳤다. 계약 규모 3억 3,000만 파운드와 견주면, 낸 법인세는 그 165분의 1에도 못 미치는 액수다. 물론 계약 총액과 한 해의 법인세 납부액을 직접 비교하는 것은 정확한 셈법이 아니다. 계약금 전부가 그해의 이익으로 잡히는 것도 아니고, 법인세는 매출이 아니라 이익에 매겨지기 때문이다. 다만 그 격차가 눈에 띄게 크다는 사실만은 이 수치들이

보여준다.

영국 하원 과학기술위원회는 별도 보고서에서, 공공 부문에서 팔란티어의 입지가 커지는 상황을 받아들이기 어려운 취약점이라고 평가했다.

독일과 스페인, 영국의 사례를 나란히 놓으면 공통된 형태가 드러난다. 세 나라 모두 팔란티어와 상당한 규모의 공공 계약을 맺었지만, 실제로 걷은 법인세는 계약 규모에 비해 크게 작았다. 세 나라의 세무당국이 각자 다른 방식으로 회계를 들여다봤음에도 결과가 비슷했다는 것은, 이 회계 구조가 특정 국가의 느슨한 감독 때문이 아니라 팔란티어가 여러 나라에 공통으로 적용하는 회계 정책 때문일 가능성을 시사한다고 CICTAR 보고서는 분석한다.

CICTAR 보고서가 예외로 꼽은 나라는 프랑스다. 보고서에 따르면 프랑스 국세청은 팔란티어가 프랑스 안에서 올린 이익을 프랑스 지사의 장부에 온전히 기록하도록 요구했고, 그 결과 팔란티어 프랑스 지사는 2024년 160만 유로의 법인세를 33퍼센트의 실효세율로 납부했다. 다른 나라의 수치와 견주면 훨씬 높은 비율이다. 이 차이가 프랑스 국세청의 적극적인 세무 집행에서 비롯됐다는 것이 보고서의 해석이다. 프랑스는 2019년부터 자국 안에서 매출을 올리는 대형 디지털 기업에 별도의 디지털서비스세를 물려 온 나라이기도 하다.

미국 대형 기술 기업을 겨냥한 이 세금 제도는 그동안 미국 정부와 여러 차례 통상 마찰을 빚었다. 팔란티어에 대한 프랑스 국세청의 집행 방식도 이런 조세 정책의 연장선에서 나온 것으로 볼 수 있다.

유럽연합 집행위원회는 개별 회원국의 세무 집행에만 기대지 않고, 다국적 기업의 과세 표준 자체를 통일하는 방안도 별도로 추진하고 있다. BEFIT이라는 이름으로 불리는 이 제안은, 유럽연합 안에서 사업하는 다국적 기업이 회원국마다 다른 방식으로 세금을 계산하는 대신 하나의 공통 기준으로 과세 소득을 산정하도록 하자는 내용을 담고 있다. 이 제안 역시 아직 유럽의회와 이사회의 심의를 거치는 단계에 있으며, CICTAR 보고서가 지적한 이전가격을 이용한 소득 이전 문제를 근본적으로 줄이려는 시도 가운데 하나로 거론된다.

이 보고서가 나온 뒤 노동계의 반응이 이어졌다. 독일 매체 랩아넷 저머니가 2026년 8월 5일 전한 바에 따르면, 국제공공노련(PSI) 사무총장 얀 빌렘 구드리아안은 공공 보건과 안전망 예산을 지키지 못하는 해외 공급업체에 국가의 핵심 조달을 맡기는 관행을 멈춰야 한다고 말했다. 같은 보도는 네덜란드 최대 노동조합 FNV 관계자의 발언도 전했는데, 공공 인프라의 혜택을 누리면서도 그에 상응하는 세금을 내지 않는 기업의 관행을 더는 두고 볼 수 없다는 내용이었다. 이런 반응을 낸 단체들은 공공 조달 입찰 규격서에 세금 납부 이력을 반영하자고 제안하고 있다.

지금까지 공공 조달은 가격과 기술 성능을 주된 평가 기준으로 삼아 왔는데, 여기에 그 기업이 실제로 얼마의 세금을 냈는지를 추가하자는 것이다. 이 제안이 실제 조달 규정에 반영됐는지는 이 책이 확인한 자료 범위 안에서는 확인되지 않는다.

이 조세 문제는 5.1에서 살펴본 투자 격차와도 맞닿아 있다. 유로스택 보고서는 유럽이 2035년까지 3,000억 유로를 마련해야 한다고 추산했고, 유럽연합이 실제로 배정한 예산은 그에 크게 못 미쳤다. CICTAR 보고서가 주장하는 것처럼 팔란티어를 비롯한 역외 기업이 유럽에서 벌어들인 이익에 걸맞은 세금을 냈다면, 그 세수가 유로스택이 요구하는 투자 재원의 일부가 될 수 있었으리라는 것이 조세 개혁을 요구하는 쪽의 주장이다. 물론 이 인과관계는 CICTAR 보고서를 지지하는 쪽의 정치적 주장이며, 이 책이 별도로 검증한 사실은 아니다.

이 조세 문제는 앞선 장에서 다룬 안보 문제와 다른 층위에서 같은 결론으로 이어진다. 제1장과 제4장이 다룬 것은 팔란티어 같은 기업에 국가의 데이터와 시스템 운영을 맡길 때 생기는 통제권의 문제였다. CICTAR 보고서가 제기하는 것은 그 계약에서 실제로 얼마의 돈이 국가 재정으로 돌아오는가라는 문제다. 이탈리아 국가사이버보안청은 이 두 문제를 함께 고려해, 국가의 핵심 조달에서 미국계 플랫폼을 배제하는 방향으로 정책을 정했다고 밝혔다.

조세와 안보라는 서로 다른 두 근거가 같은 결론을 가리키고 있다는 사실이, 유럽의 정책 입안자들이 이 문제를 미룰 수 없는 이유로 거론되고 있다.

유로스택이 요구하는 3,000억 유로도, 아르카디아와 오펜데스크를 개발하는 비용도, CICTAR가 지적한 세원도, 결국 하나의 질문으로 수렴한다. 유럽이 미국 기업에 의존하지

않는 기술 기반을 세우려 할 때, 그 기반을 세울 돈은 어디서 나오는가라는 질문이다. 은행에 잠긴 예금을 끌어내든, 이미 확보된 예산으로 소프트웨어를 개발하든, 새어 나가는 세금을 틀어막든, 세 가지 길은 모두 같은 목적지를 향한다.

시민의 입장에서 보면 이 문제는 추상적인 회계 논쟁이 아니다. 경찰서와 병원, 국방부가 낸 조달 예산은 시민의 세금에서 나온다. 그 예산의 상당 부분이 계약을 맺은 기업의 세금으로 다시 국고에 돌아오지 않는다면, 공공 서비스에 쓰일 재원은 그만큼 줄어든다. CICTAR와 폴로우더머니가 제기한 문제의 핵심은 이 순환 구조가 지금 끊겨 있다는 데 있다. 세금을 내고 그 세금으로 공공 서비스를 운영하고, 그 공공 서비스가 다시 기업의 활동을 뒷받침하는 순환이 정상적으로 작동하려면, 조달 계약을 맺은 기업이 그 나라에서 정당한 몫의 세금을 내야 한다는 전제가 성립해야 한다.

근거자료

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

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

3. Rika Baack, 'Big Data bei der Polizei', LabourNet Germany, 2026년 8월 5일.

4. ITEP, 'Palantir Pays Zero Federal Income Tax Despite Explosive Growth, Largely Due to Trump Tax Law', ITEP Reports, 2026년 3월 22일.

5. Joshua Carroll, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026년 6월 4일.

6. 영국 하원 과학기술위원회, 보고서, House of Commons, 2026년.

7. 이탈리아 국가사이버보안청, 'Sovranità digitale e IA: l'Italia tra autonomia e dipendenza', 이탈리아 정부, 2026년.

결론: 종속의 관리에서 회복력 있는 개방성으로

결론 1. 대체재가 성숙하기 전의 선언, 향후 2~3년의 리스크 구간 극복

2025년 12월 15일, 팔란티어는 프랑스 국내보안총국과 3년짜리 다년 계약을 새로 맺었다고 발표했습니다. 이 계약이 채 여섯 달도 지나지 않은 2026년 6월 16일, 프랑스 총리 세바스티앙 르코르뉘는 이 계약의 상대를 프랑스 기업 햅스비전으로 바꾸겠다고 선언했습니다. 다음 날 르몽드는 팔란티어 쪽이 갱신된 계약은 법적으로 여전히 유효하다고 주장한다고 보도했습니다. 발표와 계약 종료는 같은 사건이 아닙니다. 이 책의 1장에서 다룬 이 사례는, 유럽 정부가 앞으로 2년에서 3년 동안 관리해야 할 전환 위험이 어떤 모양을 하고 있는지를 압축해서 보여줍니다.

조달의 문제부터 살펴봐야 합니다. 프랑스 내무부는 새 프로그램을 배치하고 기존 데이터를 옮기는 데 18개월에서 24개월이 걸릴 것으로 내다봤고, 다른 보도는 계약 구조 전체의 완전한 전환이 2027년에서 2029년 사이에 걸릴 것으로 보았습니다. 로랑 뉘네즈 내무장관은 이 공백을 메우기 위해 2027년까지 팔란티어와 햅스비전을 함께 운영하는 과도기를 두겠다고 밝혔습니다. 독일에서도 같은 문제가 반복됩니다.

독일 연방헌법수호청은 2026년 5월 팔란티어 대신 아르곤OS를 조달하기로 확정했지만, 이 조달이 실제로 가동되려면 연방정보국과 연방헌법수호청의 권한을 새로 정하는 700쪽 넘는 법률 개정안이 먼저 통과되어야 합니다. 독일 연방헌법재판소는 이 법 개정의 시한을 2026년 말로 정해 두었습니다. 조달을 확정한 사실과 그 조달이 실제로 가동되는 시점은 서로 다른 절차에 묶여 있습니다.

계약의 조건 자체가 전환 속도를 결정하기도 합니다. 바덴뷔르템베르크주 내무부는 2025년 3월, 중도에 끝낼 수 있는 조항 없이 5년 동안 2,500만 유로를 지불하는 조건으로 팔란티어의 고담 프로그램 도입 계약을 맺었습니다. 주 연립정부에 참여한 녹색당 내부에서 이 계약을 즉시 중단해야 한다는 의견에 92퍼센트가 찬성했지만, 출구 조항이 없는 계약은 정치적 반대만으로 뒤집히지 않았습니다. 조달 계약에 해지 조건을 미리 넣어 두지 않으면 국가가 스스로 협상력을 잃는다는 사실을, 이 계약은 숫자로 보여줍니다.

인력과 데이터 이동의 문제는 계약서 밖에서 벌어집니다. 프랑스 국내보안총국의 요원들은 팔란티어의 화면 구성과 조작 방식에 이미 익숙해져 있고, 정보를 저장하는 방식 자체가

미국 시스템의 규격에 맞추어 짜여 있습니다. 새 프로그램으로 넘어가려면 기존 조작 방식을 새 화면에 맞추어 옮기고, 요원을 다시 교육하고, 데이터가 오가는 경로를 새로 마련하고, 진행 중인 수사가 끊기지 않도록 지키고, 실제 업무량을 견딜 수 있는지 검증하는 단계를 순서대로 밟아야 합니다. 독일 연방군도 비슷한 절차를 밟고 있습니다.

사이버·정보공간사령부의 토마스 다움 해군중장은 2026년 4월 팔란티어를 군사 클라우드 사업 pCloudBw의 후보에서 뺐다고 밝혔고, 이후 독일 기업 알마토와 베를린의 신생 기업 오크리스트 테크놀로지스, 프랑스 기업 햅스비전 세 곳이 2026년 여름 동안 실전 데이터를 연동하는 시험을 거쳤습니다. 최종 낙찰자는 2026년 말에 발표될 예정입니다. 팔란티어를 뺀 일과 누구를 새로 뽑을지는 아직 별개로 남은 문제입니다.

네덜란드는 조달 파편화라는 또 다른 형태의 위험을 안고 있습니다. 국방차관 데르크 보스베이크는 2026년 6월 2일 하원에서 팔란티어를 유럽산 대안으로 되도록 빨리 바꾸겠다고 밝히고, 완전히 동등한 수준의 대안을 찾는 데 2년을 목표로 잡고 있다고 말했습니다. 그러나 정부가 이후 하원에 낸 답변에는 구체적인 종료 시한 대신 대체안 검토와 의존도 축소라는 표현만 담겼습니다. 국방부 안에서 팔란티어와 맺은 계약이 부처별로 따로 이루어져 있어 정부 차원의 통일된 계약 목록조차 없다는 사실이 이 답변의 배경입니다.

보스베이크 차관 스스로도 지금 당장 관계를 끊으면 작전 전투 체계와 국방 병참, 정보 처리에 안보 공백이 생길 수 있다고 인정했습니다. 선언의 속도와 실행의 속도가 다르다는 사실을, 네덜란드 정부는 스스로 증언한 셈입니다.

연합작전의 영역에서는 전환의 방향이 오히려 반대로 움직입니다. 북대서양조약기구는 2025년, 팔란티어의 메이븐 스마트 시스템을 연합작전사령부에서 쓰기 위해 확보했다고 밝혔습니다. 이 확보 발표와 2026년 현재 이 체계가 실제로 어느 범위까지 가동되고 있는지는 구분해서 볼 문제로 남아 있습니다. 다만 이 책의 3장에서 짚은 대로, 국내 치안 정보 영역에서 팔란티어를 걷어내는 움직임과 군사 동맹 영역에서 팔란티어의 입지가 유지되는 흐름이 같은 시기에 나란히 벌어지고 있다는 사실은 분명합니다.

유럽연합 인공지능법의 2조와 전문 24항은 군사, 국방, 국가안보 목적의 인공지능 시스템을 규정 적용 범위에서 빼 두었습니다. 국내 정보기관의 이탈이 국방과 나토 차원의 조달까지

자동으로 끌고 가지는 않는다는 뜻입니다. 네덜란드 국방부가 나토 동맹국과 정보를 주고받으려면 같은 체계를 써야 한다는 상호운용성 요건을 전환의 걸림돌로 꼽은 이유도 여기에 있습니다. 여기에 미국 클라우드법은 미국 법인이 다루는 정보라면 서버 위치와 무관하게 미국 수사 당국이 접근할 길을 열어 둡니다. 전환이 끝나지 않은 구간에서는 이 법의 사정권도 함께 남아 있습니다.

대체 공급자의 성숙도 역시 이 전환기의 폭을 결정합니다. 햅스비전은 2019년 설립 이후 스물다섯 건 넘는 인수를 거쳐 2025년 매출 2억 유로를 기록했지만, 창립한 지 오래된 팔란티어에 비하면 여전히 성장 중인 회사입니다. 독일의 최종 후보 알마토와 오크리스트 테크놀로지스도 2026년 말에야 실전 배치 여부가 갈립니다. 유럽연합 집행위원회는 클라우드·AI 개발법을 통해 유럽 데이터센터 역량을 5년에서 7년 사이에 세 배 이상 늘려 2035년까지 기업과 공공행정 수요를 충족하겠다는 목표를 제시했습니다.

이 법은 2026년 8월 현재 집행위원회가 낸 규정 제안이며, 아직 제정되지 않았습니다. 공급 능력을 늘리는 계획의 완성 시점 자체가 이미 2030년대 중반을 바라보고 있습니다.

앤트로픽의 2026년 6월 사건은 이 모든 전환의 배경을 이룹니다. 미국 정부는 6월 12일, 외국 국적자의 페이블 5와 미토스 5 접근을 차단하라는 수출통제 지시를 앤트로픽에 내렸습니다. 접근은 이후 수출통제가 해제되며 복구되었습니다. 이 사건은 영구적인 차단이 아니라 공급이 언제든 끊길 수 있다는 가능성을 실물로 보여준 사건이었습니다. 프랑스와 독일, 네덜란드가 각자 다른 속도로 대체재를 찾는 사이, 이 가능성은 사라지지 않고 남아 있습니다.

이 책이 다루는 사례들에서 공통적으로 드러나는 것은, 선언의 날짜와 실제 전환이 끝나는 날짜 사이에 예외 없이 몇 년의 간격이 있다는 사실입니다. 그 간격을 메우는 동안 각국은 미국 기술과 유럽의 대안을 나란히 쓰는 이중 운용을 피할 수 없습니다.

근거자료

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. 저자 미상, '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. 저자 미상, '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. 저자 미상, '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. Egl⌧ Kri⌧topaityt⌧, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

8. 저자 미상, '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

결론 2. 개방성을 유지하는 회복력 있는 자립(Resilient Openness)의 길

스위스 연방보건청과 연방통계청, 연방정보기술청, 국방조달청 아르마수이스, 자금세탁방지신고사무국은 2020년부터 2024년까지 다섯 개 기관, 네 해에 걸쳐 팔란티어를 받아들이지 않기로 거듭 결정했습니다. 스위스는 프랑스나 독일처럼 이미 도입한 프로그램을 걷어내는 나라가 아닙니다. 처음부터 문턱을 넘지 못하게 막아 온 기관들이 쌓여, 지금은 새로 설득할 필요조차 크지 않은 상태에 이른 나라입니다.

보안 매체 젠데이터는 2026년 2월, 스위스가 팔란티어를 물리친 이유가 성능이 부족해서가 아니라 독점적이고 불투명한 내부 구조와 외국의 사법 관할권, 원격으로 이루어지는 업데이트 방식이 통제할 수 없는 주권 위험으로 평가되었기 때문이라고 보도했습니다. 데이터를 스위스 안에 두고 계약서에 보호 조항을 넣는 정도로는 이 위험을 충분히 막을 수 없다는 것이 스위스 쪽의 판단이었습니다. 그렇다고 스위스가 외국 기술 전체를 걸어 잠근 것은 아닙니다.

스위스가 실제로 걸러낸 것은 팔란티어라는 특정 공급자였고, 그 판단 기준은 국적이 아니라 데이터의 소재와 관할권, 업데이트 통제권이었습니다.

스페인의 조치도 비슷한 결의 선택을 보여줍니다. 스페인 총리실은 2026년 7월 1일, 통신기업 텔레포니카와 방산기업 인드라, 조선기업 나반티아 등 국영기업지주회사 산하 공기업들에 팔란티어와 새로 계약하지 말라는 지침을 내렸습니다. 이미 맺은 계약까지 무효로 하지는 않았습니다. 스페인군 정보센터가 팔란티어와 맺은 약 1,650만 유로 규모의 계약은 2026년 11월까지 그대로 이어집니다. 새 계약을 막는 일과 기존 계약을 끊는 일은 다른 문제라는 사실을, 스페인 정부는 정책의 설계 단계에서부터 인정하고 들어간 셈입니다. 반대편에는 바덴뷔르템베르크주의 사례가 있습니다.

출구 조항 없이 5년, 2,500만 유로로 묶인 이 계약은 주 연립정부 내부의 반대표 92퍼센트로도 되돌릴 수 없었습니다. 독일 연방헌법재판소도 2023년 2월, 헤센주와 함부르크주가 예측 치안에 팔란티어 기반 체계를 쓰던 근거 법률에 위헌 판결을 내리면서, 시민의 통신 기록과 개인정보를 법적 근거 없이 광범위하게 분석하는 방식이 정보자기결정권을 침해한다고 판단했습니다. 계약에 출구가 없으면 정치적 의지도, 사법부의

판단도 실행으로 이어지는 데 시간이 걸립니다.

이 사례들을 나란히 놓으면 완전한 폐쇄와 무조건적인 의존이라는 양극단이 각기 다른 방식으로 무너진다는 사실이 드러납니다. 폐쇄 쪽의 한계는 네덜란드 국방차관 데르크 보스베이크가 스스로 인정한 데서 확인됩니다. 그는 팔란티어와 지금 당장 관계를 끊으면 작전 전투 체계와 국방 병참, 정보 처리에 안보 공백이 생길 수 있다고 밝히면서도, 군사용 인공지능 분야에서는 지금 같은 수준의 유럽 대안이 없다는 사실을 함께 인정했습니다. 능력이 뒷받침되지 않는 폐쇄는 선언에 그칩니다.

반대로 의존 쪽의 한계는 2026년 6월의 앤트로픽 수출통제 사건과, 서버의 위치와 무관하게 미국 수사 당국의 접근을 허용하는 미국 클라우드법이 보여줍니다. 조약이나 계약서의 문구만으로는 이 노출을 막을 수 없습니다. 유럽연합 인공지능법이 군사, 국방, 국가안보 목적의 인공지능 시스템을 규정 적용 범위에서 빼 둔 것도, 모든 영역에 같은 규칙을 적용하는 대신 영역별로 다른 기준을 두는 쪽을 유럽연합이 이미 선택했다는 증거입니다.

유럽연합 집행위원회가 낸 클라우드·AI 개발법 제안은 이 두 극단 사이에서 유럽이 실제로 고른 길을 보여줍니다. 이 법은 2026년 8월 현재 제정된 법률이 아니라 집행위원회의 규정 제안이며, 데이터센터 역량을 5년에서 7년 사이에 세 배 이상 늘려 2035년까지 기업과 공공행정 수요를 채운다는 목표를 인공지능 대륙 실행계획의 하나로 담고 있습니다. 이 책 4장에서 살펴본 4단계 주권 보증 수준 설계와 주권 사유 해지권 조항은, 가장 민감한 영역만 골라 격리하고 나머지 영역에서는 외국 기술을 계속 조달하되 계약에서 벗어날 권리를 미리 확보해 두는 방식입니다.

바덴뷔르템베르크주가 겪은 출구 없는 계약의 문제를, 제도로 미리 막아 두려는 시도라고 볼 수 있습니다. 이 책 5장에서 다룬 프란체스카 브리아 등의 유로스택 구상 역시 비슷한 문제의식에서 출발합니다. 유럽 전역의 디지털 기반시설을 다시 짜기 위해서는 상당한 규모의 다년간 투자가 필요하다고 이 보고서는 밝히고 있습니다. 정확한 총액은 원 보고서의 세부 항목을 근거로 다시 확인해야 할 부분으로 남아 있습니다.

개방성과 자립을 동시에 쥐려는 이 접근은 아직 완결된 결과가 아니라 진행 중인 시도입니다. 그 시도가 실제로 얼마나 유효한지는 앞으로 확인될 몇 개의 구체적인 시점에

달려 있습니다. 독일 연방군은 pCloudBw 사업의 최종 공급자를 2026년 말에 정합니다. 독일 연방의회는 연방헌법재판소가 정한 시한에 맞추어 2026년 말까지 정보기관 권한을 새로 정하는 법을 처리해야 합니다. 프랑스 내무부는 2027년까지 팔란티어와 햅스비전을 함께 운영하겠다고 약속했습니다. 스페인군 정보센터의 팔란티어 계약은 2026년 11월에 끝납니다.

이 시점들이 실제로 지켜지는지, 그리고 그 자리를 채우는 유럽의 대안들이 팔란티어가 갖춘 수준의 안정성을 실전에서 증명하는지가, 폐쇄도 무조건적 의존도 아닌 이 절충안이 성립하는지를 가늠할 다음 기준입니다.

근거자료

1. 저자 미상, '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. 저자 미상, '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. Egl⊠ Kri⊠topaityt⊠, '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. 저자 미상, '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

디지털 주권의 이중 구조: 유럽의 탈(脫)팔란티어와 아메리칸 빅테크의 사슬

ISBN |

저 자 | 김경진
펴낸이 | 김경진
펴낸곳 | 김경진 변호사 출판사
출판사등록 | 2025. 3. 10. (제2025-000015호)
주 소 | 서울특별시 동대문구 전농로 91, 백일빌딩 304호
전 화 | 02-6338-1905
이메일 | kimkj008@gmail.com

가격 : 비매품

참고) 이 책의 일부 내용과 편집 과정에는 인공지능 도구의 도움을 받았습니다.

후원 안내

이 책을 잘 읽으셨으면 그리고 새로운 가치있는 지식을 얻으셨다고 판단되시면
농협 302-1096-0948-81 (예금주 김경진) 에 자발적 후원 부탁드립니다.