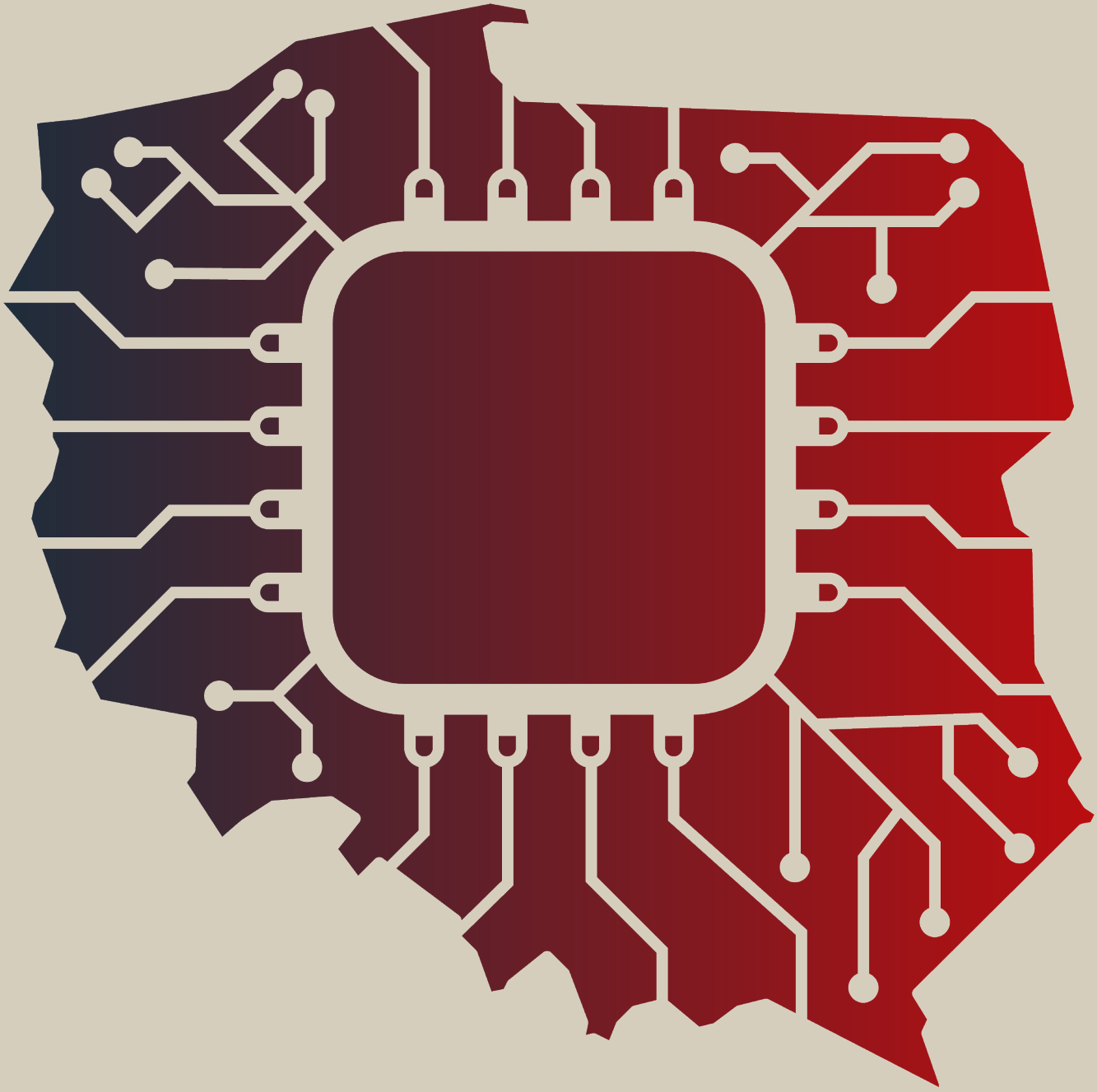
Cyfrowa racja stanu

Polska Sieć Ekonomii

Suwerenność cyfrowa jako narzędzie bezpieczeństwa, rozwoju i polityki przemysłowej państwa



Michał Myśliwiec
Maria Świetlik
Jan Oleszczuk-Zygmuntowski

Raport
Polskiej Sieci Ekonomii
dla Związku Pracodawców –
Polska Chmura

Polska Chmura

Warszawa
Lipiec 2026

Cyfrowa racja stanu. Suwerenność cyfrowa jako narzędzie bezpieczeństwa, rozwoju i polityki przemysłowej państwa. Raport Polskiej Sieci Ekonomii dla Związku Pracodawców – Polska Chmura

Zespół autorski:
Michał Myśliwiec
Maria Świetlik
Jan Oleszczuk-Zygmuntowski

Redakcja i korekta:
Aleksandra Sekuła

Wydawca:
Polska Sieć Ekonomii
Warszawa 2026
ISBN 978-83-974591-3-7

Rekomendujemy cytowanie: Myśliwiec, M., Świetlik, M., Oleszczuk-Zygmuntowski, J. (2026). *Cyfrowa racja stanu: Suwerenność cyfrowa jako narzędzie bezpieczeństwa, rozwoju i polityki przemysłowej państwa*. Raport Polskiej Sieci Ekonomii dla Związku Pracodawców – Polska Chmura. Polska Sieć Ekonomii.

Cyfrowa racja stanu

Suwerenność cyfrowa jako narzędzie bezpieczeństwa, rozwoju i polityki przemysłowej państwa

Michał Myśliwiec
Maria Świetlik
Jan Oleszczuk-Zygmuntowski

Spis treści

Kluczowe wnioski

- **Wyścig o suwerenność cyfrową już trwa, a Polska w nim nie uczestniczy**. Państwa Europy Zachodniej, Komisja Europejska oraz główni gracze globalni aktywnie budują własne ramy suwerenności i inwestują w nią środki publiczne.
- **Suwerenność cyfrowa jest kwestią bezpieczeństwa narodowego**. Chmura, systemy administracji, dane publiczne stanowią infrastrukturę krytyczną państwa i powinny być traktowane z taką samą powagą jak infrastruktura energetyczna czy transportowa.
- Unijne i polskie ramy prawne wskazują, że **ocena jurysdykcji i struktury kontrolnej dostawcy chmury i AI jest zarówno możliwa, jak i konieczna**.
- Polska potrzebuje **ambitnej polityki suwerenności cyfrowej** jako koła zamachowego nowego modelu rozwoju gospodarczego, budującego *local content*, czyli **krajowe kompetencje, miejsca pracy i przewagi konkurencyjne w gospodarce cyfrowej.**
- **Deficyt handlowy Polski w obszarze produktów cyfrowych przekroczył w 2025 roku 60 mld zł**, a do 2030 roku wydatki na import technologii cyfrowych przewyższą łączne koszty importu wszystkich surowców energetycznych.
- **W 2024 roku łączne roczne nakłady na wytworzenie i utrzymanie systemów teleinformatycznych tylko w administracji publicznej przekroczyły 7 mld zł**. Znaczna część tych środków zasila budżety zagranicznych korporacji technologicznych, nie tworząc krajowych kompetencji ani aktywów. **Przy zakładanym wzroście kosztów licencji i usług chmurowych o 12% rocznie, oznacza to w perspektywie 5 lat wzrost o 76% wydatków na tego typu zakupy.**
- Prognozowane podwyżki cen licencji na usługi AI i chmurowe będą kosztowały europejską gospodarkę **rocznie średnio dwa razy wię-**

cej niż koszty wywołane zamknięciem cieśniny Ormuz, przy założeniu, że wzrost cen za baryłkę utrzymałby się na stałym poziomie przez rok.

- Polska **nie posiada wystarczających regulacji, które gwarantowałyby bezpieczeństwo** kluczowej infrastruktury cyfrowej państwa. Brak ustawy chmurowej, niewiążący charakter obowiązujących wytycznych oraz luki w systemie certyfikacji pozostawiają administrację publiczną bez ochrony przed ingerencją obcych aktorów w krajowe systemy i dane.
- **Proponujemy kaskadowy test suwerenności jako standard stosowany w zamówieniach publicznych**. Test powinien obejmować takie kryteria jak: **ocena operacyjna** wpływu infrastruktury na funkcje państwa, **podległość jurysdykcyjna, wpływ ekonomiczny, poziom poznawczy i demokratyczny, warunki środowiskowe**.
- Kluczowe wymagania dot. technologii w zamówieniach publicznych dla infrastruktury cyfrowej o wysokiej ocenie w teście suwerenności, zapobiegające m.in. *vendor-lock-in* to: **interoperacyjność, otwarte standardy, otwarte API, oprogramowanie na wolnych licencjach (FOSS), przenoszalność danych oraz *exit capability***.
- **Zamówienia publiczne i ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa** powinny być głównymi narzędziami budowania bezpieczeństwa, tworząc realne zachęty do wyboru suwerennych rozwiązań i eliminując z postępowań dostawców, którzy nie spełniają kryteriów jurysdykcyjnych.
- Rozwój suwerenności cyfrowej wymaga także **pilnego doinwestowania krajowego ekosystemu** poprzez **programy PFR, BGK oraz edukację do wolności cyfrowej w szkołach i administracji publicznej**,
- **Ocena jurysdykcji, której podlega dostawca usług chmurowych i jego grupa kapitałowa, mieści się w materialnym zakresie art. 7 ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa**, ponieważ eksterytorialny dostęp organów państwa trzeciego do danych – sprawowany na podstawie prawa państwa trzeciego i poza

kontrolą administratora – narusza poufność wprost chronioną tym przepisem, a środki czysto techniczne pozostają wobec niego nieskuteczne. Stanowi on zatem „znane ryzyko w zakresie cyberzagrożeń" w rozumieniu art. 7, co czyni odporność na taki dostęp dopuszczalnym kryterium certyfikacji. Tym samym ujęcie kryterium jurysdykcji w schemacie krajowym wydawanym na podstawie art. 15 stanowi realizację delegacji ustawowej, nie jej przekroczenie.

Europa znajduje się obecnie w okresie intensywnych przemian regulacyjnych, technologicznych i geopolitycznych związanych z rosnącym znaczeniem suwerenności cyfrowej oraz strategicznej autonomii. W warunkach kształtowania nowych ram regulacyjnych opóźnienie działań może skutkować utrwaleniem zależności technologicznych oraz osłabieniem pozycji krajowych podmiotów nie tylko wobec globalnych dostawców technologii cyfrowych, lecz również względem państw europejskich, które już realizują polityki rozwoju własnych zdolności infrastrukturalnych.

Polityka suwerenności cyfrowej powinna być traktowana jako obszar o znaczeniu strategicznym, wykraczający poza perspektywę pojedynczych cykli wyborczych. Realizacja tego rodzaju przedsięwzięć wymaga trwałego konsensusu co do kierunku rozwoju infrastruktury cyfrowej państwa oraz konsekwencji w realizacji przyjętych celów. W przeciwnym razie kolejne zmiany priorytetów politycznych mogą prowadzić do przerywania procesów transformacyjnych, odwracania wcześniej wdrożonych reform oraz osłabienia zdolności instytucji publicznych do akumulacji wiedzy, doświadczeń i kompetencji niezbędnych do prowadzenia samodzielnej polityki technologicznej.

Wprowadzenie

Żyjemy w czasach polikryzysu i transformacji ładu światowego. Kryzys zachodniego modelu demokracji liberalnej, wojna w Ukrainie, wojna hybrydowa prowadzona przez Federację Rosyjską, rosnący protekcjonizm, zerwanie łańcuchów dostaw oraz kryzys klimatyczny wymuszają rewizję dotychczasowych polityk gospodarczych i rozumienia pojęcia bezpieczeństwa. **Epoka neoliberalnej deregulacji i bezwarunkowej globalizacji dobiegła końca, a państwa powracają do aktywnej polityki przemysłowej, wzmacniania lokalnych kompetencji oraz budowy odporności strategicznej.** Ten zwrot ku suwerenności dotyczy również sfery cyfrowej.

Polska, jako państwo, gospodarka i społeczeństwo, jest obecnie w znacznym stopniu uzależniona od globalnych dostawców technologicznych, przede wszystkim amerykańskich Big Techów i ich chińskich konkurentów. Uzależnienie to obejmuje infrastrukturę cyfrową administracji publicznej, a także usługi publiczne, w tym edukację. **Osiągnięcie trwałego bezpieczeństwa państwa wymaga jednak zapewnienia odpowiedniego poziomu suwerenności cyfrowej i traktowania infrastruktury cyfrowej jako infrastruktury krytycznej**. Tymczasem krajowe regulacje w tym obszarze nadal koncentrują się przede wszystkim na cyberbezpieczeństwie i odporności operacyjnej, w niewystarczającym stopniu uwzględniając problem zależności technologicznych, ekonomicznych, ekologicznych i jurysdykcyjnych.

Równocześnie **trwa globalny wyścig o suwerenność technologiczną i cyfrową**. Komisja Europejska, a także państwa takie jak Francja i Niemcy, wdrażają ambitne strategie w celu zwiększenia kontroli nad kluczową infrastrukturą, danymi, jednocześnie inwestując w rozwój lokalnych kompetencji technologicznych i zdolności przemysłowych w tym obszarze. Można spodziewać się, że **w wyniku tych działań wkrótce powstaną europejskie firmy rywalizujące z Big Techami**

o prymat na europejskim rynku, także w obszarze usług dla administracji publicznej krajów członkowskich.

Polska nie może pozostać biernym obserwatorem tych procesów. **Konieczne jest podjęcie pilnych i zdecydowanych działań na rzecz budowy własnej suwerenności cyfrowej**, aby zachować zdolność do samodzielnego kształtowania polityk publicznych, ochrony interesów gospodarczych oraz zapewnienia bezpieczeństwa państwa.

Wyścig suwerennościowy trwa, a dla Polski może być unikatową szansą – kołem zamachowym nowego modelu rozwoju – przesuwając naszą pozycję z kraju półperyferyjnego ku centrum światowej gospodarki.

Rozdział I
Triada bezpieczeństwo – suwerenność – infrastruktura

Bezpieczeństwo i suwerenność cyfrowa pozostają w ścisłej zależności – suwerenność cyfrowa stanowi fundament umożliwiający skuteczną realizację bezpieczeństwa. Dlatego niezwykle istotne jest właściwe zmapowanie wszystkich warstw tworzących tę suwerenność. Na potrzeby niniejszej analizy definiujemy suwerenność cyfrową w następujący sposób:

> **Suwerenność cyfrowa** oznacza **zdolność państwa i jego instytucji do egzekwowania swoich praw oraz interesów, w tym bezpieczeństwa narodowego, w kontekście infrastruktury cyfrowej** przy jednoczesnym zachowaniu konkurencyjnego poziomu produktów i usług[1].

1.1. Osiem wymiarów suwerenności cyfrowej

Według *Schematu suwerennej chmury* (*Cloud Sovereignty Framework*) (Komisja Europejska, 2025) przedstawionego w 2025 r. przez Komisję Europejską, suwerenność cyfrowa może być opisana poprzez osiem kategorii[2]. Są to:

1 Zgodnie z definicją zaproponowaną w raporcie *Polska suwerenna cyfrowo*, suwerenność cyfrowa oznacza ogólnie zdolność państw, organizacji międzynarodowych, a także każdego użytkownika i użytkowniczki z osobna do egzekwowania swoich praw oraz wpływania na platformy cyfrowe i firmy technologiczne zgodnie z własnymi potrzebami społecznymi i rozwojowymi (Wawrzyniak i in., 2020).

2 *Cloud Sovereignty Framework*, wersja 1.2.1, 20 października 2025 r.; dokument wymienia osiem celów, od SOV-1 do SOV-8, które tu przedstawiamy jako osiem kategorii.

1.1.1. Suwerenność strategiczna

Dotyczy tego, kto faktycznie kontroluje dostawcę i gdzie powstaje wartość. Obejmuje m.in. strukturę własnościową, wpływ podmiotów spoza UE, inwestycje i miejsca pracy w UE oraz odporność na polityczne naciski zewnętrzne.

1.1.2. Suwerenność prawna i jurysdykcyjna

Sprawdza, jakiemu prawu podlega dostawca i czy istnieje ryzyko działania przepisów spoza UE. Obejmuje ochronę przed eksterytorialnym dostępem do danych oraz zapewnienie stosowania prawa UE.

1.1.3. Suwerenność danych i AI

Koncentruje się na kontroli nad danymi, kluczami szyfrującymi i modelami AI. Zakłada, że klient powinien mieć realną kontrolę nad dostępem do danych, ich usuwaniem oraz lokalizacją przetwarzania danych i modeli AI w UE.

1.1.4. Suwerenność łańcucha dostaw

Dotyczy pochodzenia sprzętu, firmware'u, oprogramowania i komponentów krytycznych. Wskazuje na problematyczną zależność od dostawców spoza UE oraz podkreśla znaczenie przejrzystości i możliwości audytu całego łańcucha dostaw.

1.1.5. Suwerenność operacyjna

Ocenia, czy europejskie podmioty mogą samodzielnie operować usługą bez krytycznej zależności od dostawcy spoza UE. Ważne są tu możliwość migracji, unikanie *vendor lock-in* oraz niezależne zarządzanie usługą.

1.1.6. Suwerenność technologiczna

Obejmuje wykorzystanie otwartych standardów, interoperacyjność, dostępność oprogramowania na licencjach zezwalających na audyt, modyfikację i redystrybucję oraz możliwość integracji bez uzależnienia od zamkniętych technologii jednego dostawcy.

1.1.7. Suwerenność środowiskowa

Ocenia efektywność energetyczną infrastruktury chmurowej, wpływ środowiskowy oraz podejście do cyrkularności i trwałości infrastruktury IT.

1.1.8. Suwerenność bezpieczeństwa i zgodności

Dotyczy zgodności z europejskimi regulacjami, lokalizacji SOC-ów i zespołów bezpieczeństwa, procedur reagowania na incydenty oraz możliwości prowadzenia europejskich audytów bezpieczeństwa.

1.2. Suwerenność cyfrowa a infrastruktura krytyczna państwa

Pojęcie infrastruktury krytycznej jest ugruntowane zarówno w prawie krajowym, jak i unijnym. Zgodnie z definicją, zawartą w polskiej ustawie o zarządzaniu kryzysowym, infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Definicja ta koncentruje się przede wszystkim na ciągłości świadczenia usług oraz odporności systemów technicznych.

Choć obowiązujące regulacje Unii Europejskiej dotyczące infrastruktury krytycznej nie posługują się wprost pojęciem suwerenności cyfrowej, to coraz wyraźniej rozszerzają zakres ochrony na infrastrukturę cyfrową, w tym centra danych, usługi chmurowe, sieci telekomunikacyjne oraz

systemy teleinformatyczne. Zarówno **dyrektywa NIS2**, jak i **dyrektywa CER** (por. rozdział *Unijne ramy regulacyjne*) opierają się na założeniu, że **zakłócenie funkcjonowania tych systemów** (np. usług chmurowych czy centrów danych) **może wywoływać skutki porównywalne z awariami tradycyjnej infrastruktury krytycznej**. W rezultacie **zdolność państwa do utrzymania kontroli nad kluczowymi zasobami cyfrowymi jest coraz częściej analizowana jako jeden z praktycznych wymiarów suwerenności cyfrowej**, rozumianej jako zdolność do autonomicznego i bezpiecznego wykonywania podstawowych funkcji publicznych w warunkach rosnącej zależności od infrastruktury informacyjnej.

Proponujemy zatem definicję, zgodnie z którą infrastruktura krytyczna nie jest wyłącznie kategorią techniczną, lecz strukturą warunkującą ciągłość funkcjonowania państwa jako złożonego systemu.

> **Infrastruktura krytyczna** rozumiana jest przez nas jako zbiór powiązanych systemów technicznych, organizacyjnych, cyfrowych i naturalnych, których funkcjonowanie warunkuje zdolność państwa do reprodukcji trzech kluczowych wymiarów jego działania:
>
> - **władzy publicznej** (rozumianej jako zdolność do stanowienia, egzekwowania i implementacji decyzji politycznych, w tym z zakresu bezpieczeństwa),
> - **wiedzy instytucjonalnej** (zdolności do wytwarzania, przetwarzania i utrzymywania informacji niezbędnych do podejmowania decyzji oraz wiedzy o tym procesie),
> - **zasobów naturalnych i infrastrukturalnych** (obejmujących zarówno infrastrukturę fizyczną, jak i cyfrową oraz ich łańcuchy dostaw, a także ekosystemy).

Zdolność państwa do samodzielnego zarządzania infrastrukturą krytyczną oraz podejmowania niezależnych decyzji technologicznych stanowi fundament samostanowienia narodów, a zatem istnienia nie-

podległego państwa. Kontrola nad infrastrukturą krytyczną wyznacza bowiem granice rzeczywistej autonomii decyzyjnej wspólnoty: jeśli kluczowe systemy, od łączności i energetyki po administrację publiczną i usługi danych, pozostają pod kontrolą podmiotów zewnętrznych lub są od nich krytycznie zależne, żaden z wymiarów suwerenności nie może być w pełni zrealizowany.

Utrata faktycznej kontroli nad infrastrukturą krytyczną oznacza w praktyce utratę zdolności do egzekwowania własnych praw i interesów w przestrzeni cyfrowej – niezależnie od obowiązujących regulacji prawnych.

Rozdział II
Zagrożenia dla suwerenności cyfrowej

W debacie o suwerenności cyfrowej uwaga często koncentruje się na kwestiach technicznych, takich jak cyberbezpieczeństwo, lokalizacja danych czy wybór konkretnych technologii. W rzeczywistości problem ma znacznie szerszy charakter. Współczesna infrastruktura cyfrowa jest kontrolowana przez niewielką grupę globalnych korporacji technologicznych, które dysponują bezprecedensową skalą zasobów, danych, wpływu gospodarczego i politycznego. Powoduje to powstanie nowych form zależności, obejmujących nie tylko sferę technologiczną, lecz również bezpieczeństwo państwa, autonomię regulacyjną oraz zdolność do budowania krajowych kompetencji i wartości gospodarczej.

Niniejszy rozdział przedstawia trzy kluczowe wymiary tego problemu. Po pierwsze, analizuje rolę Big Techów i hiperskalerów jako podmiotów kontrolujących znaczną część globalnej infrastruktury cyfrowej. Po drugie, omawia ryzyka wynikające z podlegania zagranicznym jurysdykcjom oraz ich konsekwencje dla bezpieczeństwa narodowego i funkcjonowania administracji publicznej. Po trzecie, wskazuje ekonomiczne koszty zależności technologicznej, obejmujące zarówno bezpośrednie wydatki publiczne, jak i długoterminowy odpływ kapitału, kompetencji oraz możliwości rozwojowych poza krajową gospodarkę.

2.1. Big Techy i hiperskalerzy

Big Techy to globalne korporacje technologiczne kontrolujące kluczowe elementy infrastruktury cyfrowej – chmurę obliczeniową, AI, platformy danych, systemy operacyjne, oprogramowania biurowe i ekosystemy aplikacyjne. Problemem z perspektywy państwa jest fakt, że strategiczne obszary funkcjonowania administracji i gospodarki stają się zależne od

podmiotów pozostających poza krajową kontrolą operacyjną, prawną i polityczną, co wprost ogranicza suwerenność Polski.

Nadmierna zależność od Big Techów prowadzi również do utraty kompetencji krajowych oraz trwałego odpływu środków publicznych poza krajowy ekosystem. **Państwo traci zdolność samodzielnego rozwijania i utrzymywania kluczowych usług cyfrowych, a lokalny rynek IT zostaje sprowadzony do roli podwykonawcy lub sprzedawcy zagranicznych systemów.**

Co więcej, dzięki korzyściom skali zagraniczne firmy monopolizują zamówienia publiczne i doprowadzają do zjawiska *vendor lock-in*[3], czyli uzależnienia klienta od swoich produktów i usług. Dzieje się tak, ponieważ koszty, które musiałaby ponieść administracja w związku ze zmianą dostawcy są wyższe niż pozostania w obrębie jego systemu (***exit capability***). Monopolista może podwyższać wówczas marże bez poprawiania jakości swoich rozwiązań, jednocześnie nie pozwalając rozwinąć się krajowej konkurencji.

Przykładem takiej praktyki są działania firmy Microsoft. Korporacja systematycznie podnosi ceny licencji w programie SPLA (Service Provider License Agreement) – umowach, na podstawie których dostawcy usług hostingowych oraz instytucje publiczne korzystają z oprogramowania serwerowego Microsoftu. W 2025 roku podwyżki wyniosły od 10% dla podstawowych produktów serwerowych, przez 11% dla systemów klasy ERP z rodziny Dynamics, aż do 17% w przypadku starszych wersji Dynamics AX. Analogiczne podwyżki miały miejsce rok wcześniej i są zapowiadane na kolejne lata (Paul, 2024; Carlson, 2024). Strategia Microsoft polega przy tym na **podnoszeniu kosztów oprogramowania instalowanego lokalnie przy równoczesnym utrzymywaniu stabilnych cen usług chmurowych** – co tworzy ekonomiczny przymus stop-

3 *vendor lock in* – sytuacja, w której użytkownik jest uzależniony od jednego dostawcy technologii, produktu lub usługi, i zmiana dostawcy wiąże się z wysokimi kosztami, trudnościami technicznymi lub ryzykiem zakłócenia działalności. Zjawisko to często występuje w obszarze usług chmurowych, gdy wykorzystanie specyficznych rozwiązań, formatów danych lub infrastruktury jednego dostawcy utrudnia migrację do alternatywnych rozwiązań.

niowej migracji klientów do platform chmurowych producenta. Efektem jest nie tylko rosnący rachunek, lecz także coraz głębsze uzależnienie od jednego dostawcy.

Innym przykładem działań firmy Microsoft jest jej polityka cenowa w przypadku pakietu Microsoft Office 365. Na początku pandemii COVID-19, w marcu 2020 r., koncern zaoferował organizacjom nieposiadającym dotąd licencji na program Teams sześciomiesięczny bezpłatny dostęp do licencji próbnej Office 365 E1, dającej dostęp do pełnej funkcjonalności (Endicott, 2020). W sierpniu 2021 r. Microsoft ogłosił podwyżkę cen komercyjnych planów Microsoft 365, która objęła większość planów biznesowych oraz Enterprise wzrostami średnio około 15% w zależności od planu (Spataro, 2021). Kolejna podwyżka została ogłoszona w grudniu 2025 r. i wchodzi w życie 1 lipca 2026 r., obejmując niemal **wszystkie plany komercyjne wzrostami cen sięgającymi nawet 33%**, przy czym kluczowe plany Business i Enterprise podrożeją o 8–17% (Microsoft, 2026).

Najdrastyczniejszym przykładem tego zjawiska jest podwyżka cen po zmianie właściciela firmy VMware, jednego z najważniejszych dostawców oprogramowania do wirtualizacji i infrastruktury centrów danych. Po przejęciu spółki przez Broadcom w listopadzie 2023 roku **tysiące organizacji na całym świecie otrzymały oferty odnowienia licencji z podwyżkami rzędu 800–1500%** (Udhayakumar, 2026). Broadcom zlikwidował licencje wieczyste i elastyczne modele *pay-as-you-go*, zmuszając klientów do obowiązkowych trzyletnich subskrypcji z odgórnie narzuconymi cenami i pakietami różnych usług, niezależnymi od ich faktycznego wykorzystania. **Jednostronnie wypowiedział też obowiązujące umowy licencyjne**, w tym takie, które obowiązywały przez ponad 10 lat (Udhayakumar, 2026).

Szersza skala tego zjawiska również jest mierzalna. Zgodnie z wyliczeniami firmy konsultingowej Asterès **w latach 2024-2026 koszty licencji na usługi AI i chmurowe wzrosły średnio o 8,7% rocznie, a ich dalszy wzrost szacowany jest na 12% w najbliższych 5 latach** (Asterès, 2026). Co więcej, wzrost wydatków na usługi chmurowe i oprogramo-

wanie będzie kosztował europejską gospodarkę 0,6 punktu procentowego PKB rocznie do 2030 r. **Dodatkowe koszty szacowane są na 140 mld euro rocznie, z czego 93 mld euro trwale opuszczą europejską gospodarkę, wypierając wydatki u dostawców europejskich oraz inwestycje i nakłady na badania i rozwój.** Modelując efekty domina tego spadku popytu, Asterès szacuje łączne straty na 205 mld euro w obrotach, 107 mld euro w wartości dodanej i 1,4 mln miejsc pracy. Dla porównania: roczny średni koszt tych podwyżek przekracza cały roczny budżet UE i odpowiada ponad dwukrotności kwot zainwestowanych w innowacje i badania w ramach Horyzontu Europa przez siedem lat. **Koszt ten jest też dwukrotnie wyższy niż szacowane skutki szoku naftowego wywołanego zamknięciem cieśniny Ormuz, gdyby ceny za baryłkę utrzymały się na wysokim poziomie przez rok.**

2.2. Bezpieczeństwo narodowe a eksterytorialne jurysdykcje

Przekazywanie kluczowych usług cyfrowych podmiotom funkcjonującym poza polską i europejską jurysdykcją wiąże się z szeregiem zagrożeń dla bezpieczeństwa państwa oraz suwerenności cyfrowej. Dotyczy to szczególnie usług chmurowych, infrastruktury danych oraz systemów wykorzystywanych przez administrację publiczną.

Należy podkreślić, że **zagrożenie wynika z możliwości sprawowania kontroli nad danymi i usługą przez podmiot podlegający jurysdykcji państwa trzeciego, niezależnie od fizycznej lokalizacji infrastruktury**. Jeśli np. dane przechowywane są na serwerach w Polsce, ale właścicielem czy operatorem infrastruktury cyfrowej jest firma podlegająca prawu państwa trzeciego, to nie można uznać tych danych za wolne od ryzyka ujawnienia organom innego, także pozaunijnego, państwa.

W praktyce **kontrola nad infrastrukturą cyfrową obejmuje nie tylko fizyczne serwery, lecz również szereg warstw stosu technologicznego**, takich jak na przykład: system operacyjny i warstwa wirtualizacji (np. *hypervisor*), oprogramowanie chmurowe i orkiestracyjne (IaaS/PaaS), mechanizmy zarządzania kluczami kryptograficznymi, systemy

uwierzytelniania i zarządzania tożsamością, mechanizmy aktualizacji i utrzymania oprogramowania, systemy telemetrii, logowania i diagnostyki, panel administracyjny dostawcy, a także relacje z podwykonawcami i globalnym łańcuchem dostaw. W przypadku usług opartych o tzw. sztuczną inteligencję istotnym elementem są również modele oraz powiązane z nimi dane i procesy uczenia, o ile są one dostarczane i kontrolowane przez operatora usługi.

2.2.1. FISA: eksterytorialna inwigilacja

Ustawa o Nadzorze Wywiadowczym (Foreign Intelligence Surveillance Act [FISA], 1978) jest jednym z kluczowych instrumentów eksterytorialnego oddziaływania jurysdykcji amerykańskiej na globalne przepływy danych. Amerykańskie służby wywiadowcze **uzurpują sobie prawo do pozyskiwania danych dotyczących osób niebędących obywatelami USA znajdujących się poza terytorium Stanów Zjednoczonych**, w ramach programów nadzoru prowadzonych z wykorzystaniem usług cyfrowych globalnych dostawców, takich jak operatorzy chmur obliczeniowych czy platform internetowych. W praktyce oznacza to, że podmioty podlegające jurysdykcji USA są zmuszone do udostępniania danych, również jeśli są one fizycznie przechowywane na terenie Unii Europejskiej.

Istotnym momentem w globalnej debacie o zakresie stosowania FISA było ujawnienie w 2013 roku przez Edwarda Snowdena, byłego współpracownika amerykańskich służb wywiadowczych, zasięgu tej inwigilacji. Opublikowane przez niego **dokumenty National Security Agency (NSA) pokazały skalę operacyjnego wykorzystania mechanizmów nadzoru, w tym programów opartych na FISA, do masowego pozyskiwania danych** z globalnych systemów telekomunikacyjnych i platform cyfrowych. Ujawnienia te unaoczniły, że instrumenty takie, jak dodana w 2008 r. sekcja 1881a (obecnie 702), która zezwoliła na inwigilację obywateli nieamerykańskich także poza terytorium Stanów, nie mają charakteru teoretycznego, lecz stanowią podstawę szeroko zakrojonych praktyk, obejmujących cały glob. Co więcej, **firmy amerykańskie**

w zasadzie nie mają możliwości odmówienia przekazania dostępu do danych obcokrajowców, a jednocześnie są chronione przed odpowiedzialnością za takie działanie. Sprawa Snowdena stała się punktem zwrotnym w międzynarodowej debacie o prywatności i suwerenności danych, a jednocześnie jednym z kluczowych odniesień w ocenie ryzyk związanych z eksterytorialnym dostępem do infrastruktury cyfrowej. Doprowadziła także do **unieważnienia porozumienia Bezpieczna Przystań (Safe Harbor)**, które miało regulować zasady przekazywania danych obywatelek i obywateli UE do USA.

Sekcja 702 FISA (pierwotnie sekcja 1881a) była także istotnym punktem odniesienia w orzecznictwie Trybunału Sprawiedliwości UE (TSUE). W sprawie *Schrems II*[4] (2020) Trybunał uznał, że **amerykańskie regulacje dotyczące dostępu służb do danych nie gwarantują obywatelom UE odpowiedniego poziomu ochrony prywatności**, co doprowadziło do **unieważnienia również porozumienia Tarcza Prywatności (Privacy Shield)**, pozostawiając kwestie transferu danych bez nowej regulacji aż do 2023 r., kiedy to zakończyły się negocjacje pomiędzy administracją USA i Komisja Europejską w tej sprawie.

Wraz z przyjęciem decyzji Komisji Europejskiej w sprawie EU–US Data Privacy Framework (DPF) powstał nowy mechanizm uznania adekwatności ochrony danych osobowych w Stanach Zjednoczonych dla certyfikowanych podmiotów. DPF ma zapewnić „zasadniczo równoważny" poziom ochrony jak w RODO przy jednoczesnym ułatwieniu transferów komercyjnych. W rezultacie **transfer danych do USA nie jest zablokowany, jednak pozostaje uzależniony od spełnienia określonych warunków**, w tym dobrowolnej certyfikacji.

Obecnie decyzja DPF została zakwestionowana przez posła Philippe'a Latombe, który wniósł sprawę do TUSE po ujawnieniu, że Komisja Eu-

4 Sprawa *Schrems II* dotyczyła skargi austriackiego aktywisty Maxa Schremsa kwestionującej legalność przekazywania danych osobowych europejskich użytkowników Facebooka do Stanów Zjednoczonych w kontekście dostępu amerykańskich służb do tych danych na podstawie przepisów dotyczących nadzoru elektronicznego.

ropejska korzysta z usług Amazon Web Services i Microsoft do przetwarzania danych osobowych pracowników i urzędniczek, co może naruszać przepisy rozporządzenia (UE) 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych. Obecnie DPF pozostaje w mocy mimo trwającej procedury odwoławczej przed TSUE.

2.2.2. CLOUD Act: naruszenie poufności i integralności danych

Innym aktem, który umożliwia władzom USA żądanie dostępu do danych posiadanych przez amerykańskie przedsiębiorstwa, niezależnie od miejsca ich przechowywania, jest CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018). O ile FISA obejmuje działalność agencji wywiadowczych, to **CLOUD Act dotyczy przede wszystkim postępowań prowadzonych przez organy ścigania** i wynikających z tego uprawnień do dostępu do danych przechowywanych przez dostawców usług elektronicznych i chmurowych.

Akt powstał po głośnym sporze między rządem USA a Microsoft. Amerykańskie władze zażądały wydania danych użytkownika znajdujących się na serwerze w Irlandii, natomiast Microsoft argumentował, że amerykański nakaz nie może działać poza terytorium USA. Zanim sprawa została ostatecznie rozstrzygnięta przez sąd, Kongres uchwalił CLOUD Act, który de facto przesądził tę kwestię: amerykański dostawca usług (oraz podmioty zależne kapitałowo) może zostać **zobowiązany do przekazania danych znajdujących się pod jego „posiadaniem, pieczą lub kontrolą”** (*possession, custody or control*), niezależnie od miejsca ich fizycznego przechowywania.

W świetle obowiązującego stanu prawnego należy przyjąć, że **dostawca podlegający jurysdykcji Stanów Zjednoczonych nie jest w stanie zagwarantować poufności i integralności danych powierzonych przez podmiot publiczny**. CLOUD Act umożliwia bowiem organom amerykańskim żądanie wydania danych niezależnie od fizycznej lokalizacji serwerów w Unii Europejskiej oraz bez wiedzy i zgody administratora, co stanowi przekazanie danych do państwa trzeciego pozbawione podstawy

w rozdziale V RODO i nieusuwalne wyłącznie środkami technicznymi po stronie dostawcy. **Obowiązywanie Data Privacy Framework nie usuwa tego ryzyka**, gdyż reguluje ono jedynie komercyjne przekazywanie danych, a nie ogranicza dostępu służb USA do danych na potrzeby bezpieczeństwa narodowego. W tych okolicznościach **zamawiający publiczny, działając jako administrator danych,** jest na podstawie zasady rozliczalności oraz obowiązku zapewnienia bezpieczeństwa przetwarzania (art. 5 ust. 1 lit. f i art. 32 RODO), a także w oparciu o ramy europejskiej i krajowej certyfikacji cyberbezpieczeństwa ustanowione ustawą z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa, nie tylko uprawniony, lecz wręcz **zobowiązany do ustanowienia w postępowaniu proporcjonalnego, neutralnego co do pochodzenia wykonawcy warunku odporności na pozaprawny dostęp organów państw trzecich**. Skutkiem prawnym powinno być wykluczenie z udziału w zamówieniu podmiotów, które warunkowi temu, ze względu na podleganie CLOUD Act, sprostać nie mogą.

2.2.3. Sankcje jako narzędzie represji politycznych

Uzależnienie od zagranicznych dostawców ogranicza również zdolność państwa do samodzielnego zarządzania infrastrukturą krytyczną oraz podejmowania niezależnych decyzji technologicznych. W sytuacjach kryzysowych lub napięć geopolitycznych może prowadzić to do utraty części kontroli operacyjnej nad kluczowymi usługami publicznymi i systemami państwowymi.

> **Wolne i otwarte oprogramowanie (Free and Open Source Software, FOSS)** to termin obejmujący dwa różne nurty. **Wolne oprogramowanie (Free Software)** to zarówno kategoria oprogramowania, jak i ruch społeczno-polityczny, który definiuje tzw. **cztery wolności osoby użytkującej** oprogramowanie opracowane przez Free Software Foundation (System Operacyjny GNU, 2026):

Wolność do uruchamiania programu jak chcecie, w dowolnym celu (wolność 0).
Wolność do analizowania, jak działa program, i zmieniania go, aby robił, co i jak potrzebujecie (wolność 1). Warunkiem koniecznym jest dostęp do kodu źródłowego.
Wolność do rozpowszechniania kopii, byście mogli pomóc innym (wolność 2).
Wolność do udoskonalania programu i publicznego rozpowszechniania własnych ulepszeń, dzięki czemu może z nich skorzystać cała społeczność (wolność 3). Warunkiem koniecznym jest tu dostęp do kodu źródłowego.
W tym ujęciu kluczowe znaczenie ma nie tylko techniczna dostępność kodu, lecz przede wszystkim normatywne założenie, że użytkowniczki i użytkownicy powinni **posiadać pełną kontrolę nad oprogramowaniem jako dobrem wspólnym**.
Szczególną kategorię FOSS stanowi oprogramowanie udostępniane na licencjach typu ***copyleft*** (np. GNU GPL), które wymagają zachowania tych samych wolności również w przypadku modyfikacji i dystrybucji kodu.
Otwarte oprogramowanie (Open Source Software) to oprogramowanie, którego kod źródłowy jest publicznie dostępny, a jego licencja spełnia kryteria definicji *open source* opracowanej przez Open Source Initiative. Podejście *open source* koncentruje się na transparentności kodu oraz efektywności modelu rozwoju oprogramowania poprzez współpracę wielu niezależnych podmiotów.

Wymownym przykładem jest przypadek **Międzynarodowego Trybunału Karnego w Hadze**. W maju 2025 roku, po tym jak administracja Trumpa objęła sankcjami głównego prokuratora MTK Karima Khana, Khan **utracił dostęp do swojej służbowej poczty elektronicznej hostowanej przez Microsoft** – wywołując w Europie poważne obawy o bezpieczeństwo cyfrowe („ICC to ditch Microsoft following US sanctions", 2025). MTK

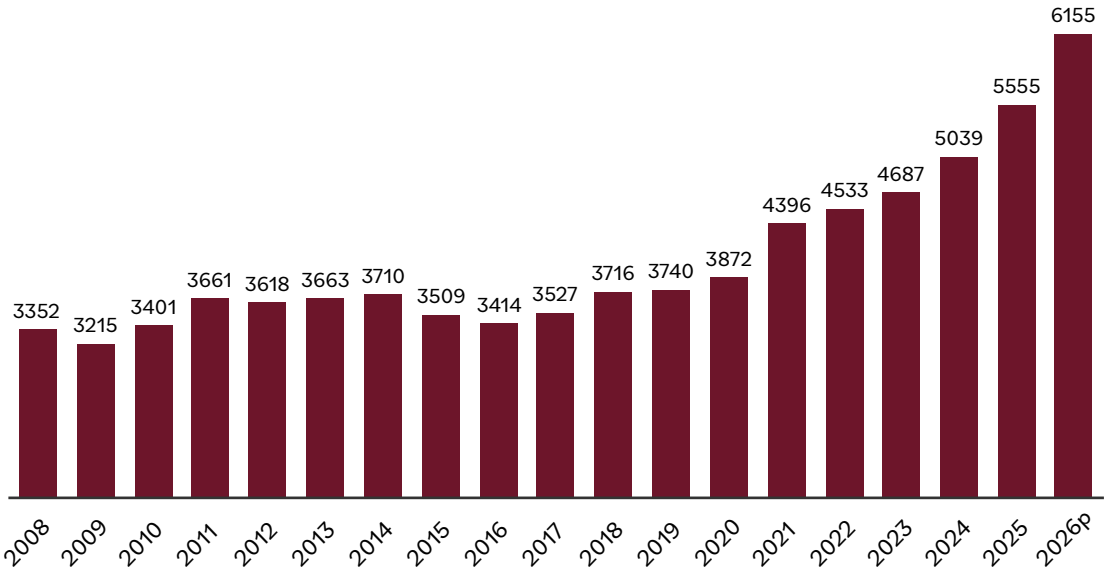
zdecydował się ostatecznie na zerwanie współpracy z Microsoftem i przejście na alternatywny zestaw usług (stos) opartych o wolne lub otwarte oprogramowanie (Free and Open Source Software, FOSS) w pakiecie **openDesk** – rozwijany w ramach niemieckiej inicjatywy na rzecz suwerenności cyfrowej i szeroko stosowany w niemieckiej administracji publicznej.

Innym przykładem problematyczności wykorzystywania usług cyfrowych w czasach geopolitycznych napięć jest przypadek dostawcy usług komunikacyjnych, firmy **Zoom**. Zoom **uniemożliwił swoim użytkownikom transmisję wydarzeń upamiętniających masakrę na placu Tiananmen**, co uzasadnił koniecznością dostosowania się do regulacji chińskich (Kuo i Davidson, 2020). Jest to dobra ilustracja ryzyka związanego z eksterytorialnością jurysdykcji. Globalne platformy mogą egzekwować ograniczenia wynikające z różnych reżimów prawnych, co bezpośrednio wpływa na swobodę korzystania z ich usług użytkownikom w innych jurysdykcjach.

2.3. Koszty ekonomiczne

Rynek cyfrowy rozwija się dynamicznie, podobnie jak jego wpływ na budżety firm, państw czy UE.

Wykres 1. Globalne wydatki na rozwiązania cyfrowe (w miliardach dolarów)



Źródło: Asterès. (2026). *From technological dependency to economic capture: The cost of cloud & software services inflation to Europe*.

Brak suwerenności cyfrowej wiąże się nie tylko z zagrożeniami dla bezpieczeństwa państwa, ale również z bardzo wysokimi kosztami ekonomicznymi ponoszonymi przez administrację publiczną – w postaci bezpośrednich wydatków oraz utraconych korzyści (na przykład nie szacuje się **potencjalnych zysków, jakie wynikałyby dla gospodarki czy bezpieczeństwa z rozwijania lokalnych alternatywnych rozwiązań technologicznych**, tymczasem istotne jest analizowanie decyzji zakupowych i inwestycyjnych w długoterminowej perspektywie).

Problem ten pogłębia się z czasem, w miarę oligopolizacji danego rynku usług. **Brak konkurencji daje dostawcom przewagę rynkową, która pozwala narzucać coraz wyższe marże, zgodnie z działaniem mechanizmu tzw. renty monopolowej** (oligopolowej).

Rentą taką określa się dochody uzyskiwane przez podmioty posiadające pozycję monopolistyczną (lub oligopolistyczną), które wynikają albo z ograniczenia dostępu do określonych zasobów, albo z jego unikatowych cech. Może ona przyjmować różne formy – od rent wynikających z prawnie chronionej własności intelektualnej (np. patenty i prawa autorskie), przez de facto monopole firm kontrolujących standardy rynkowe (jak Microsoft w przypadku oprogramowania biurowego czy Intel w architekturze procesorów), aż po tzw. monopole naturalne w sektorach takich jak energetyka, kolej czy telekomunikacja.

Szczególnie **istotnym współczesnym źródłem rent monopolowych jest efekt sieci w platformach cyfrowych**, gdzie firmy takie jak Google, Facebook czy Amazon czerpią przewagę z dominacji ekosystemów użytkowników i danych. Opłaty pobierane przez duże platformy, takie jak Google Play czy Apple App Store, w analizach antymonopolowych wskazywane bywają jako przykład rent monopolowych właśnie ze względu na zdolność tych firm do narzucania warunków rynkowych w środowisku ograniczonej konkurencji.

Efektem tego procesu są strategie biznesowe dużych firm, które można porównać z **dumpingiem cenowym**, który jest formą **nadużycia pozycji dominującej** i **zabronionym czynem nieuczciwej konkurencji.**

Początkowo korporacje technologiczne oferują swoje usługi po bardzo atrakcyjnych cenach, zachęcając instytucje do migracji danych i procesów do własnych systemów. Jednak po osiągnięciu dominującej pozycji rynkowej dostawcy uzyskują możliwość stopniowego podnoszenia cen, ograniczania interoperacyjności oraz zwiększania zależności klientów od własnego ekosystemu technologicznego. Dobrym przykładem jest wspomniany już Microsoft, który podczas pandemii COVID-19 oferował usługę Teams za darmo na 6 miesięcy w celu przyzwyczajenia użytkowników do swojego produktu, aby później wprowadzać regularne podwyżki cen pakietów.

Eksperci z firmy konsultacyjnej Elée (2025) szacują, że do 2028 roku średni roczny wzrost kosztów oprogramowania najczęściej wykorzystywanego przez firmy i administrację (Microsoft, Oracle, SAP, Salesforce, itp.) wyniesie od +12% do +14% rocznie. Oznaczałoby to skumulowany wzrost w ciągu czterech lat o co najmniej 57%.

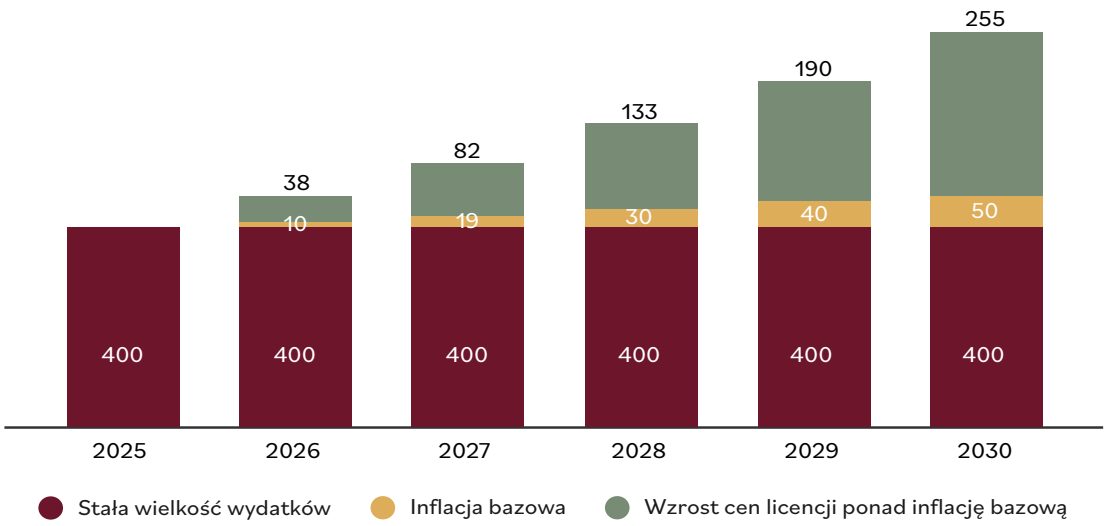
Francuskie stowarzyszenie reprezentujące największe francuskie firmy i administrację publiczną, Cigref, opublikowało analizę *Technological dependence on American software and cloud services: an estimate of the economic consequences in Europe*, w której wskazało, że **z 400 mld EUR, które europejskie organizacje wydały w 2024 r. na usługi chmurowe i oprogramowanie, 330 mld trafiło do firm amerykańskich** (Asterès, 2025). Co więcej, **80% tej wartości (265 miliardów euro) jest wytwarzana w USA, gdzie odpowiada szacunkowo za stworzenie (bezpośrednio lub nie) około 2 milionów miejsc pracy**. Zgodnie z zawartą w raporcie prognozą, **gdyby do 2035 r. udało się zatrzymać w europejskiej gospodarce zaledwie 15% obecnych wydatków na usługi chmurowe i oprogramowanie, mogłoby to przełożyć się na:**

- **37 mld wartości dodanej,**
- **16 mld dodatkowych wpływów do budżetów publicznych,**
- **utworzenie około 463 tys. miejsc pracy (bezpośrednich, pośrednich oraz indukowanych).**

Pokazuje to, że rozwój europejskich kompetencji i rozwiązań cyfrowych jest zarówno kwestią bezpieczeństwa i suwerenności, jak i istotnym impulsem gospodarczym.

Pod koniec maja 2026 r. Cigref przedstawił przeprowadzoną na jego zlecenie przez firmę Asterès kolejną analizę, która pokazuje **niepokojący trend wzrostu kosztów usług chmurowych i licencji na oprogramowanie** w ujęciu makro (Asterès, 2026). Do swoich wcześniejszych wyliczeń badacze dodali uśredniony wskaźnik inflacyjny cen licencji 12% rocznie w okresie 2026–2030[5]. Oznaczałoby to dodatkowy wzrost wydatków o średnio 140 mld euro rocznie w ciągu tych 5 lat.

Wykres 2. Rozbicie prognozowanych wydatków na oprogramowanie chmurowe ponoszonych przez europejskie organizacje w latach 2025–2030 (w miliardach euro)



Źródło: Asterès. (2026). *From technological dependency to economic capture: The cost of cloud & software services inflation to Europe*.

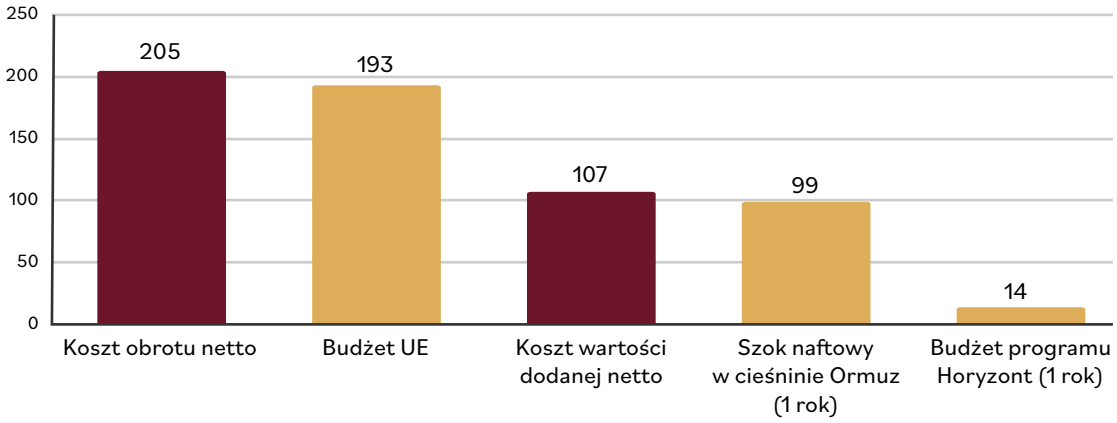
Aby pokryć te dodatkowe koszty, organizacje priorytetowo traktują redukcję innych wydatków cyfrowych (tak zadeklarowało 47% respondentów, dyrektorów ds. cyfryzacji z europejskich firm i administracji publicznej, przebadanych przez Asterès) lub zwiększenie ogólnego budżetu cyfrowego (33% odpowiedzi), kosztem usług zewnętrznych, za-

5 Por. Elée. (2025). *Note stratégique. Tendances du marché logiciels & cloud*.

kupów sprzętu, wydatków na badania i rozwój, rekrutacji i wynagrodzeń. Dla 71% z nich pięcioletnia trajektoria inflacji jest nie do udźwignięcia. Zdecydowana większość respondentów (93%) uważa, że podwyżki cen są nieuzasadnione w świetle obserwowanych zysków[6].

Dokonując estymacji, autorzy twierdzą, że **zjawisko tej nadmiernej inflacji ograniczy potencjał europejskiej gospodarki o około 107 mld euro wartości dodanej rocznie – co odpowiada 0,6 proc. PKB – oraz doprowadzi do utraty około 1,4 mln potencjalnych miejsc pracy do 2030 roku**.

Wykres 3. Roczny koszt wzrostu ceł dla europejskiej gospodarki pod względem obrotów i wartości dodanej w porównaniu z wydatkami publicznymi i szokiem cenowym na rynku ropy naftowej (w miliardach euro)



Źródło: Asterès. (2026). *From technological dependency to economic capture: The cost of cloud & software services inflation to Europe*.

Można tu dodać, że **szczególnie niepokojące jest wskazane przez respondentów ograniczenie wydatków na badania i rozwój** – racjonalne w skali przedsiębiorstwa działanie w skali państwa oznaczać może pogłębianie zależności od zakupu innowacyjnych technologii produkowanych poza Europą. (Jak szacują badacze, średni roczny koszt obrotu

6 Użycie tzw. sztucznej inteligencji, wskazywane przez dostawców jako uzasadnienie podwyżek cen, generuje wymierny wzrost produktywności tylko dla 23% respondentów. 52% z nich, nawet jeśli dostrzega potencjał, nie jest w stanie go oszacować, a 25% obserwuje wyłącznie negatywne lub nieistotne skutki. Zdecydowana większość respondentów (93%) uważa te podwyżki cen za nieuzasadnione w świetle obserwowanych korzyści (Asterès, 2026)

w ciągu pięciu lat wynikający z tych podwyżek cen przekroczyłby zatem roczny budżet UE i stanowiłby w ciągu jednego roku ponad dwukrotność kwot zainwestowanych w innowacje i badania w ramach programu Horyzont Europa w ciągu siedmiu lat).

Oceniając koszty zakupów technologicznych, należy zatem uwzględnić nie tylko cenę samej usługi, ale również to, gdzie trafia wydany pieniądz publiczny. **Złotówka wydana u krajowego dostawcy pozostaje w polskiej gospodarce**: zasila budżet państwa przez podatki, tworzy miejsca pracy w Polsce i finansuje inwestycje na krajowym rynku. Złotówka wydana u zagranicznego korporacyjnego dostawcy w przeważającej części opuszcza polską gospodarkę – trafia do zagranicznych akcjonariuszy, budżetów innych państw i globalnych struktur kapitałowych. Prowadzi to do znacznego **deficytu w bilansie handlu produktami cyfrowymi**, co omawiamy szerzej w części poświęconej Polsce.

Opłaty za licencje i usługi oferowane przez zagraniczne korporacje często przekraczają koszty stworzenia oraz utrzymania krajowych rozwiązań technologicznych w perspektywie jednego roku. Np. we Francji **żandarmeria dzięki zmianie systemu operacyjnego z własnościowego na Linux oszczędza 2 miliony euro rocznie na samych licencjach** (Canonical Ubuntu, 2010), a miasto Monachium, według szacunków, w ciągu 7 lat zaoszczędziło w sumie 11 milionów euro na przejściu z Windows na LiMux (Adach, 2024). Przykłady te szerzej omawiamy w rozdziale poświęconym dobrym praktykom stosowanym za granicą. Poziom oszczędności dla względnie niewielkich jednostek administracyjnych pokazuje, że przy wprowadzeniu własnych rozwiązań dla całego państwa można uzyskać dużo wyższe oszczędności wynikające z samego efektu skali.

Innym, niewidocznym, wymiarem ekonomicznym związanym z suwerennością cyfrową jest łańcuch wartości danych. Szacunki Web3 Foundation wskazują, że przeciętny użytkownik w Europie generuje rocznie ok. 1,6 tys. USD (ok. 5 904 zł) wartości komercyjnej. **Estymacja dla całej populacji Polski wynosi 60,8 mld USD (ok. 224,4 mld zł) utraconej wartości rocznie**.

Tabela 1: Wartość komercyjna generowana przez użytkowników według terytoriów

Terytorium	Na osobę na rok	Na osobę przez całe życie	Na osobę przez całe życie (z uwzględnieniem inflacji)
Globalnie	2 561 zł	153 632 zł	457 862 zł
USA	24 217 zł	1 453 066 zł	3 067 500 zł
Ameryka Północna	17 133 zł	1 027 996 zł	2 170 155 zł
Wielka Brytania i Europa	5 919 zł	355 129 zł	698 904 zł
Reszta świata	978 zł	58 667 zł	174 921 zł

Źródło: Oprac. własne na podstawie: Web3 Foundation (2026). *The Hidden Price of Free: What Your Data Is Really Worth. The Personal Economics of Big Tech and AI* (wartości przeliczone po kursie USD/PLN = 3.69).

Ze względu na dominację usług cyfrowych oferowanych przez firmy zagraniczne można mówić o systematycznym i strukturalnym **„wycieku wartości z danych obywateli”**, polegającym na tym, że ta wartość ekonomiczna jest w znaczącym stopniu przechwytywana przez Big Techy.

Ocena efektywności ekonomicznej rozwiązań cyfrowych powinna uwzględniać całkowity koszt posiadania[7]**, koszty uzależnienia od dostawcy oraz koszty utraconych korzyści dla gospodarki.** Cena licencji stanowi jedynie jeden z elementów tego rachunku. Szczególne znaczenie mają koszty związane z *vendor lock-in*, które mogą prowadzić do ograniczenia konkurencji, wzrostu cen oraz utraty zdolności do samodzielnego kształtowania infrastruktury cyfrowej. Z kolei analiza efektywności wydatków publicznych na technologię musi uwzględniać wpływ na bilans w handlu produktami cyfrowymi.

7 Całkowity koszt posiadania (ang. *total cost of ownership*,TCO) to sposób oceny realnych kosztów danego rozwiązania technologicznego w całym jego cyklu życia, a nie tylko przez pryzmat ceny zakupu lub licencji. W przypadku systemów IT obejmuje m.in.: koszty zakupu licencji lub usług, wdrożenia i integracji z istniejącą infrastrukturą, utrzymania, wsparcia technicznego, szkoleń użytkowników i administratorów, aktualizacji i modernizacji systemu, migracji danych i zmiany dostawcy (tzw. *exit costs*), ryzyka, np. awarii, przestojów czy uzależnienia od jednego dostawcy (Stephens, 2024).

2.4. Międzynarodowe regulacje handlowe

Okolicznością, którą należy wziąć pod uwagę przy projektowaniu zmian regulacyjnych obejmujących handel międzynarodowy oraz relacje z inwestorami z innych państw jest system przywilejów dla inwestorów zagranicznych, który ogranicza suwerenność UE, jak i krajów członkowskich we wprowadzaniu nowych polityk i decyzji.

Bilateralne umowy inwestycyjne (ang. *Bilateral Investment Treaties*, BIT) oraz klauzule inwestycyjne w umowach o wolnym handlu (ang. *Free Trade Agreements*, FTA) stanowią międzynarodowy reżim ochrony inwestorów zagranicznych, który umożliwia im dochodzenie roszczeń przeciwko państwom przed trybunałami arbitrażowymi w ramach mechanizmu ISDS (*Investor-State Dispute Settlement*). Mechanizm ten pozwala inwestorowi pominąć sądy krajowe i kierować spór bezpośrednio na poziom międzynarodowy, najczęściej w oparciu o zarzuty naruszenia standardów takich jak sprawiedliwe i równe traktowanie, zakaz wywłaszczenia pośredniego czy zakaz dyskryminacji. W praktyce oznacza to, że zmiany regulacyjne państwa – w tym dotyczące infrastruktury cyfrowej, telekomunikacji czy ochrony danych – mogą być oceniane jako ingerencja w „uzasadnione oczekiwania inwestora".

W orzecznictwie arbitrażowym występują sprawy wygrane zarówno przez inwestorów, jak i przez państwa. W sprawie z powództwa Vattenfall państwo niemieckie zostało pozwane w związku z zaostrzeniem regulacji środowiskowych dla energetyki, co pokazuje, że zmiany polityki publicznej w sektorach infrastrukturalnych mogą generować wysokie ryzyko arbitrażowe. Z kolei w części spraw państwa skutecznie broniły swoich decyzji – na przykład w sporach takich jak Juvel and Bithell przeciw Polsce w sprawie dot. firmy Sferia, w której trybunał uznał, że decyzja UKE nie może być uznana za wywłaszczenie (Ministerstwo Cyfryzacji, 2019).

Na tym gruncie wskazuje się również na tzw. efekt ochładzający (ang. *chilling effect*). Oznacza on sytuację, w której państwa w obawie przed pozwami ograniczają zakres lub tempo reform, nawet jeśli uzna-

ją je za konieczne z punktu widzenia interesu publicznego. Efekt taki może być wywołany poprzez pojawiające się w przestrzeni medialnej ostrzeżenia kierowane pod adresem państw. Na przykład w reakcji na projekt nowelizacji przepisów o krajowym systemie cyberbezpieczeństwa Huawei skierował do polskiego rządu pismo, w którym wskazał na potencjalnie dyskryminacyjny charakter regulacji i zastrzegł możliwość wszczęcia postępowania arbitrażowego (Takagi, 2025).

Ryzyko sporów inwestycyjnych nie powinno jednak prowadzić do rezygnacji przez państwa z realizacji uzasadnionych celów publicznych. Zarówno praktyka arbitrażowa, jak i orzecznictwo międzynarodowe potwierdzają, że państwa zachowują prawo do regulowania obszarów związanych z bezpieczeństwem, zdrowiem publicznym, ochroną konsumentów czy infrastrukturą krytyczną pod warunkiem, że środki te są proporcjonalne, niedyskryminacyjne i odpowiednio uzasadnione.

W warunkach rosnącej zależności technologicznej oraz nasilającej się rywalizacji geopolitycznej szczególnego znaczenia nabiera zdolność państwa do podejmowania strategicznych decyzji regulacyjnych nawet w sytuacji potencjalnej presji ze strony podmiotów prywatnych.

Rozdział III
Unijne ramy regulacyjne

Na poziomie prawa Unii Europejskiej można wyróżnić kilka odrębnych reżimów regulacyjnych odnoszących się do infrastruktury cyfrowej, które jednak nie tworzą jednolitego systemu klasyfikacji infrastruktury pod względem jej krytyczności.

3.1. Zasady niedyskryminacji i proporcjonalności w prawie unijnym

Instrumenty polityki suwerenności cyfrowej muszą być interpretowane w świetle prawa pierwotnego Unii Europejskiej, w szczególności art. 4 ust. 2 *Traktatu o Unii Europejskiej* (TUE), który chroni podstawowe funkcje państwa, w tym bezpieczeństwo narodowe, stanowiąc gwarancję suwerenności krajów członkowskich. Z kolei przepisy *Traktatu o funkcjonowaniu Unii Europejskiej* (TFUE) wprowadzają zasadę, że rynek wewnętrzny Unii opiera się m.in. na swobodzie przedsiębiorczości (art. 49 TFUE) i swobodzie świadczenia usług (art. 56 TFUE) oraz swobodzie przepływu kapitału (art. 63 TFUE). Zgodnie z art. 26 TFUE swobody te tworzą jednolity obszar gospodarczy bez barier wewnętrznych, co stanowi podstawowy punkt odniesienia dla oceny dopuszczalności wszelkich instrumentów polityki suwerenności cyfrowej w Unii Europejskiej. Jednocześnie TFUE przewiduje możliwość ograniczenia swobód rynku wewnętrznego (w tym praw cudzoziemców, swobody usług) ze względu na porządek publiczny i bezpieczeństwo (m.in. art. 52, 62 oraz 346 TFUE).

> **Artykuł 346 [Derogacja w zakresie bezpieczeństwa i obronności]**
> 1. Postanowienia Traktatów nie stanowią przeszkody w stosowaniu następujących reguł:

> a) żadne Państwo Członkowskie nie ma obowiązku udzielania informacji, których ujawnienie uznaje za sprzeczne z podstawowymi interesami jego bezpieczeństwa;
> b) każde Państwo Członkowskie może podejmować środki, jakie uważa za konieczne w celu ochrony podstawowych interesów jego bezpieczeństwa, a które odnoszą się do produkcji lub handlu bronią, amunicją lub materiałami wojennymi; środki takie nie mogą negatywnie wpływać na warunki konkurencji na rynku wewnętrznym w odniesieniu do produktów, które nie są przeznaczone wyłącznie do celów wojskowych.

Każde takie ograniczenie podlega ponadto ocenie proporcjonalności ukształtowanej przez orzecznictwo TSUE (w szczególności w sprawie C-55/94 Gebhard). Czteroelementowy **test oceny dopuszczalności krajowych ograniczeń swobód rynku wewnętrznego** zakłada, że środek krajowy może być uznany za zgodny z prawem UE, jeżeli:

- jest stosowany w sposób niedyskryminujący,
- uzasadniony jest nadrzędnymi względami interesu publicznego,
- jest odpowiedni do osiągnięcia zamierzonego celu,
- nie wykracza poza to, co jest konieczne do jego osiągnięcia

Jednocześnie najnowsze orzecznictwo TSUE wskazuje na konieczność unikania środków dyskryminacyjnych oraz generalnych, niezindywidualizowanych ograniczeń wobec dostawców z innych państw członkowskich. Trybunał podkreśla, że zarówno środki oparte na kryterium pochodzenia kapitału (por. sprawa C-106/22 Xella), jak i regulacje o charakterze ogólnym i abstrakcyjnym (por. sprawa C-376/22 Google Ireland), podlegają ścisłej kontroli pod kątem zgodności z zasadą niedyskryminacji oraz proporcjonalności, w szczególności w celu wykluczenia ich protekcjonistycznego charakteru.

3.2. Kluczowe dyrektywy dotyczące infrastruktury cyfrowej i inne akty

W obszarze cyberbezpieczeństwa kluczowe znaczenie mają dyrektywa NIS2 (*Network and Information Systems Directive*2) (Dyrektywa PE i Rady UE 2022/2555)) oraz dyrektywa CER (*Critical Entities Resilience*) (Dyrektywa PE i Rady UE 2022/2557). NIS2 ustanawia ramy zarządzania ryzykiem cyberbezpieczeństwa oraz obowiązki w zakresie ochrony sieci i systemów informacyjnych w podmiotach uznanych za istotne dla funkcjonowania usług publicznych i gospodarki. Dyrektywa CER koncentruje się na odporności podmiotów krytycznych na zagrożenia o charakterze fizycznym, organizacyjnym i operacyjnym. W Polsce implementację tych ram stanowi ustawa o krajowym systemie cyberbezpieczeństwa, która określa obowiązki operatorów usług kluczowych oraz instytucji publicznych w zakresie zarządzania incydentami cyberbezpieczeństwa.

W obszarze usług cyfrowych i rynków cyfrowych obowiązują również: Akt o usługach cyfrowych (DSA), Akt o rynkach cyfrowych (DMA) oraz Akt w sprawie sztucznej inteligencji (AI Act). DSA i DMA obejmują swoim zakresem funkcjonowanie platform cyfrowych oraz warunki konkurencji na rynku usług cyfrowych, natomiast AI Act wprowadza podejście oparte na ocenie ryzyka dla systemów tzw. sztucznej inteligencji, nakładając określone obowiązki na dostawców systemów wysokiego ryzyka oraz modeli ogólnego przeznaczenia.

W obszarze polityki przemysłowej istotne znaczenie ma Europejski Akt w sprawie chipów (EU Chips Act), którego celem jest wzmocnienie zdolności produkcyjnych Unii Europejskiej w zakresie półprzewodników, zwiększenie odporności łańcuchów dostaw.

Kwestia *vendor-lock-in* i konieczności zapewnienia przenoszalności danych i *exit capability* została ujęta w rozporządzeniu Data Act (2023/2854), które wprowadza obowiązek zapewnienia przenoszalności danych oraz usług przetwarzania w chmurze, a także stopniowo ogranicza możliwość pobierania opłat za proces migracji i transfer danych (tzw. *switching costs* i *egress fees*), z pełnym stosowaniem kluczowych obowiązków w tym zakresie od 12 stycznia 2027 r. Regulacja

ta opiera się na założeniu, że **zapewnienie realnej możliwości zmiany dostawcy usług przetwarzania danych stanowi istotny element funkcjonowania konkurencyjnego rynku usług cyfrowych**.

Na poziomie polityk i strategii Unii Europejskiej funkcjonują dokumenty i inicjatywy o charakterze programowym, które nie mają charakteru wiążącego prawa, lecz wyznaczają kierunki rozwoju regulacyjnego i gospodarczego. Do najważniejszych należy Europejska Strategia w zakresie danych (Komisja Europejska, 2020), która zakłada rozwój jednolitego rynku danych poprzez tworzenie tzw. europejskich przestrzeni danych (*data spaces*) oraz wzmacnianie interoperacyjności i wymiany danych w gospodarce cyfrowej. Tego typu inicjatywą jest Gaia-X, będąca konsorcjum (formalnie międzynarodową organizacją non-profit) mającym na celu rozwój wspólnych ram architektonicznych i zasad dla federacyjnych usług chmurowych. Gaia-X nie stanowi infrastruktury operacyjnej ani systemu prawnego, lecz inicjatywę koordynacyjną i standaryzacyjną. Z tego powodu nie jest to skuteczne narzędzie do tworzenia alternatywnej oferty czy zmniejszania poziomu uzależnienia.

Komplementarnym instrumentem operacjonalizującym koncepcję suwerenności cyfrowej jest *Cloud Sovereignty Framework*, opublikowany przez Komisję Europejską w październiku 2025 r. Dokument ten ustanawia jednolitą metodykę oceny suwerenności dostawców usług chmurowych, opartą na ośmiu celach suwerennościowych oraz na mechanizmie ewaluacyjnym: poziomach Sovereignty Effective Assurance Level (SEAL-0–SEAL-4) oraz ilościowym wskaźniku Sovereignty Score. Praktyczne zastosowanie tej metodyki nastąpiło w kwietniu 2026 r., gdy Komisja Europejska, w ramach systemu zakupowego Cloud III Dynamic Purchasing System, udzieliła pierwszego w historii instytucji unijnych zamówienia na usługi chmurowe uwzględniającego kryteria suwerennościowe, o wartości 180 mln euro w okresie sześcioletnim, na rzecz czterech europejskich konsorcjów dostawców. W odróżnieniu od Gaia-X, *Cloud Sovereignty Framework* stanowi zatem instrument o bezpośrednim znaczeniu operacyjnym dla zamówień publicznych,

niemniej – podobnie jak inne inicjatywy o charakterze programowym – nie ma charakteru prawnie wiążącego.

Równolegle rozwijany jest *Europejski schemat certyfikacji bezpieczeństwa usług chmurowych* (*EU Cloud Services Security Certification Scheme*, EUCS). Pierwszy projekt EUCS opublikowano w grudniu 2020 r., ale od tego czasu prace nad nim pozostają w stanie wieloletniego impasu, wywołanego skutecznym sprzeciwem organizacji branżowych reprezentujących głównie dostawców z państw trzecich wobec wymogu suwerenności (lokalizacji danych i krajowości kapitału) – w efekcie ostatnia wersja schematu usunęła ten wymóg dla najwyższego poziomu zapewnienia (High+). Odpowiedzią na zaistniały impas jest opracowanie przez Komisję Europejską *Aktu w sprawie rozwoju chmury obliczeniowej i sztucznej inteligencji* (*Cloud and AI Development Act*; CADA), przedstawionego 3 czerwca 2026 r.

3.3. CADA: Cloud and AI Development Act

3 czerwca 2026 roku Komisja Europejska opublikowała projekt rozporządzenia ustanawiającego ramy dla wzmocnienia europejskiego ekosystemu chmurowego i AI – *Cloud and AI Development Act* (CADA). Jest to dokument o fundamentalnym znaczeniu dla całej dyskusji o regulacjach chmurowych w Europie, w tym w Polsce.

Po pierwsze, CADA ma zastąpić dotychczasowy projekt EUCS. Jego pojawienie się potwierdza, że Komisja Europejska porzuca ścieżkę czysto technicznej certyfikacji, unikającej uznania realnych źródeł zagrożenia, na rzecz kompleksowego podejścia suwerennościowego łączącego wymogi bezpieczeństwa i tworzenia warunków do rozwoju europejskich zdolności technologicznych. W tym kontekście **oczekiwanie na finalizację EUCS nie może stanowić wystarczającego uzasadnienia dla dalszego odkładania krajowych inicjatyw certyfikacyjnych.**

Po drugie, CADA wprowadza cztery poziomy zapewnienia bezpieczeństwa (*Union Assurance Levels* 1–4), które jako pierwsze w euro-

pejskich ramach regulacyjnych wprost uwzględniają kryteria suwerennościowe. Poziomy obejmują swym zakresem całość ekosystemu, od podstawowych wymogów lokalizacyjnych aż po pełną niezależność łańcucha dostaw, dostosowując wymagania do wrażliwości danych i charakteru obsługiwanej infrastruktury.

Tabela 2: Poziomy zapewnienia bezpieczeństwa dla dostawców usług chmurowych według projektu CADA

Poziom	1	2	3	4
Przeznaczenie	Ogólne usługi sektora publicznego	Podwyższone ryzyko, wrażliwe dane publiczne	Infrastruktura krytyczna i dane niejawne	Obronność i bezpieczeństwo narodowe
Kluczowe wymogi	Dostawca z główną siedzibą w UE; dane klientów wyłącznie w UE; infrastruktura co do zasady w UE; outsourcing wsparcia technicznego poza UE dopuszczalny przy wdrożeniu środków gwarancyjnych; transparentność i nadzór nad podwykonawcami; zgodność z aktualnymi standardami cyberbezpieczeństwa	Wymogi z poziomu 1 i ponadto personel w UE; wsparcie techniczne i operacyjne wyłącznie z UE; dane nie mogą służyć do trenowania AI podmiotów z państw trzecich; certyfikat cyberbezpieczeństwa co najmniej znaczący; udokumentowany rejestr składników oprogramowania (SBOM); dostawca może podlegać kontroli z państwa trzeciego, ale musi wykazać skuteczne środki neutralizujące tę kontrolę	Wymogi z poziomu 2 i ponadto personel wyłącznie spośród obywateli UE (z poświadczeniami bezpieczeństwa tam, gdzie wymagane); dostawca i podwykonawcy co do zasady nie podlegają kontroli z państw trzecich – wyjątek możliwy wyłącznie na podstawie aktu wykonawczego Komisji z art. 19	Wszystkie wymogi poziomu 3 bez żadnych wyjątków i ponadto certyfikat cyberbezpieczeństwa na poziomie wysokim; żaden podmiot z państwa trzeciego nie może sprawować efektywnej kontroli nad komponentami oprogramowania używanymi w usłudze (w tym nad ich rozwojem, utrzymaniem i aktualizacjami bezpieczeństwa)

Źródło: Oprac. własne.

Załącznik III do CADA szczegółowo określa wymagania audytowe dla każdego poziomu zapewnienia bezpieczeństwa. Obejmują one weryfikację struktury własnościowej dostawcy, aż do ustalenia beneficjenta rzeczywistego i ostatecznego właściciela, a także lokalizacji infrastruktury, personelu i danych oraz łańcucha dostaw oprogramowania. **Komisja Europejska wprost potwierdza tym samym, że ocena jurysdykcji i struktury kontrolnej dostawcy jest nie tylko możliwa, ale konieczna**,

i może być przeprowadzana przez wyspecjalizowane jednostki audytowe bez udziału służb specjalnych.

Fakt, że **kryteria jurysdykcyjne znalazły się w samym sercu projektu CADA, jako warunek konieczny wyższych poziomów zapewnienia bezpieczeństwa**, podlegający formalnemu audytowi, rozstrzyga spór o ich dopuszczalność. Nie są to postulaty polityczne ani bariery handlowe, lecz uznane przez Komisję Europejską narzędzia oceny ryzyka, które **muszą być uwzględniane przy projektowaniu regulacji chmurowych**.

W tym kontekście należy również odróżnić funkcję europejskich schematów certyfikacji cyberbezpieczeństwa, wynikających z art. 57 Cybersecurity Act, od szerszych instrumentów polityki przemysłowej Unii Europejskiej. O ile EUCS stanowi schemat certyfikacji cyberbezpieczeństwa usług chmurowych służący harmonizacji ich oceny w ramach rynku wewnętrznego UE, o tyle projektowane rozporządzenie CADA wpisuje się w szerszą logikę wzmacniania europejskich zdolności technologicznych oraz redukcji strategicznych zależności w sektorze cyfrowym. Oznacza to, że **krajowe instrumenty polityki suwerennościowej funkcjonują na odmiennym poziomie regulacyjnym niż unijne schematy certyfikacji i mogą pełnić wobec nich funkcję komplementarną**, szczególnie w obszarach wykraczających poza zakres harmonizacji unijnej. Polska może zatem tworzyć i rozwijać krajowe systemy certyfikacji w obszarach, których UE nie uregulowała i stosować je w zamówieniach publicznych.

Rozdział IV
Suwerenność cyfrowa w Polsce

4.1. Ile płacimy za uzależnienie?

W 2025 roku **deficyt handlowy Polski w obszarze produktów cyfrowych przekroczył zgodnie z szacunkami 60 mld zł, a do 2030 roku wydatki na import produktów cyfrowych mogą przewyższyć łączne koszty importu wszystkich surowców energetycznych** (Oleszczuk-Zygmuntowski i in., 2025). Z jednej strony można postrzegać to jako efekt transformacji energetycznej i ograniczania zależności od paliw kopalnych, z drugiej jednak stanowi to wyraźny sygnał słabości obecnego modelu gospodarczego oraz rosnącego uzależnienia od zagranicznych technologii.

Nie dotyczy to wyłącznie administracji publicznej, lecz całej polskiej gospodarki. Skala **importu usług cyfrowych pokazuje, jak krajowe przedsiębiorstwa i instytucje są uzależnione od zagranicznych rozwiązań technologicznych**. W praktyce oznacza to, że Polska eksportuje fizyczne produkty, pracę i usługi, a w zamian importuje produkty cyfrowe oraz dostęp do zagranicznej infrastruktury technologicznej. Innymi słowy, sprzedajemy atomy za bity.

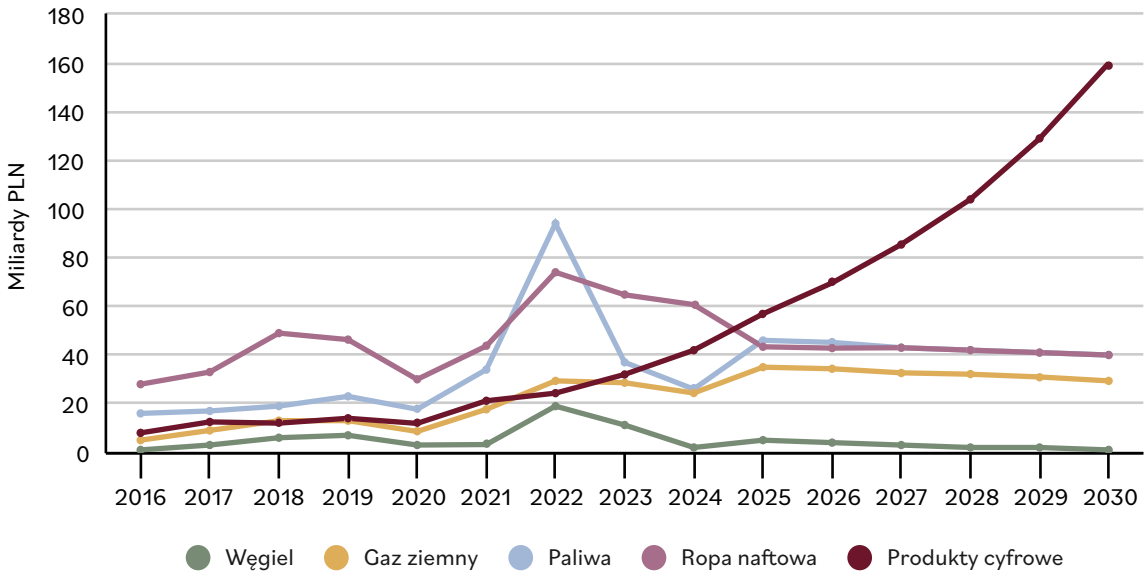
Brak jest publicznie dostępnych danych o wydatkach administracji na zakup infrastruktury cyfrowej. W odpowiedzi na interpelację posła Marka Matuszewskiego, która ukazała się 25 maja 2026 roku, Sekretarz Stanu w Ministerstwie Cyfryzacji, Dariusz Standerski poinformował, że w 2024 roku łączny koszt netto poniesiony na wytworzenie systemów teleinformatycznych w centralnych podmiotach administracji publicznej wyniósł 5,5 mld zł, a na ich utrzymanie i rozbudowę – kolejne 1,5 mld zł[8].

8 „Ministerstwo Cyfryzacji w ramach Systemu Inwentaryzacji Systemów Teleinformatycznych zbiera informacje z centralnych podmiotów administracji publicznej dotyczące łącznych kosztów netto poniesionych na wytworzenie systemów, oraz informacje dotyczące łącznych kosztów netto poniesionych na utrzymanie i rozbudowę uruchomionych systemów. Dane są

Oznacza to, że **Państwo wydało przynajmniej 7 mld złotych na systemy teleinformatyczne w 2024 roku**.

Dane te należy jednak traktować z dużą ostrożnością: dotyczą wyłącznie centralnych podmiotów administracji publicznej raportujących do Systemu Inwentaryzacji Systemów Teleinformatycznych, a więc pomijają samorządy, sądy, służby i szereg innych instytucji publicznych. Odpowiedź nie zawiera szczegółowych informacji o wydatkach na infrastrukturę chmurową, licencje na oprogramowanie czy subskrypcje usług SaaS – czyli o kategoriach kosztów bezpośrednio związanych z zależnością od zewnętrznych dostawców i zamkniętych systemów. Co równie istotne, z odpowiedzi nie wynika w ogóle, jaka część tych wydatków trafia do podmiotów zagranicznych, a jaka do polskich lub unijnych dostawców.

Wykres 4. Import netto produktów cyfrowych i paliw kopalnych



Źródło: Oleszczuk-Zygmuntowski, J. (2025). *Cyfrowy bilans Polski. Jak zmienić uzależnienie w suwerenność*

zbierane w formie informacji w SIST za poprzedni rok rozliczeniowy.

Z Rocznego sprawozdania Ministra Cyfryzacji z wykonania w 2025 r. obowiązków, o których mowa w art. 20gb ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, przez podmioty realizujące zadania publiczne, prezentującego dane za 2024 r. wynika:

- łączny koszt netto poniesiony na wytworzenie systemów wyniósł 5 535,0 mln zł
- łączny koszt netto poniesiony na utrzymanie i rozbudowę uruchomionych systemów wyniósł 1 472,4 mln zł." (Standerski, 2026b).

4.2. Ustawa o KSC i KSCC

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) z 2026 r., implementująca dyrektywę NIS2, rozszerzyła obowiązki związane z cyberbezpieczeństwem, zarządzaniem ryzykiem oraz bezpieczeństwem łańcucha dostaw, **nie ustanowiła jednak kompleksowych zasad dotyczących przetwarzania danych publicznych w chmurze, zwłaszcza w zakresie danych wrażliwych i infrastruktury o znaczeniu strategicznym.**

Ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (KSCC) (Dz.U. 2025 poz. 1017) weszła w życie jako akt uzupełniający stosowanie unijnego rozporządzenia 2019/881 w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (tzw. aktu o cyberbezpieczeństwie). Ustawa określa organizację krajowego systemu certyfikacji oraz zadania i obowiązki podmiotów wchodzących w jego skład, w tym ministra właściwego do spraw informatyzacji, pełniącego funkcję krajowego organu ds. certyfikacji cyberbezpieczeństwa, a także jednostek oceniających zgodność oraz podmiotów nadzorowanych przez ministra. Ustanawia ona ramy proceduralne dla wydawania certyfikatów krajowych, obejmujących produkty, usługi i procesy ICT[9], usługi zarządzane w zakresie bezpieczeństwa, systemy zarządzania cyberbezpieczeństwem oraz kwalifikacje osób fizycznych. W art. 7 określa ogólne kryterium materialne udzielania certyfikatu, obejmujące zapewnienie dostępności, autentyczności, integralności oraz poufności przetwarzanych danych. Szczegółowe wymogi pozwalające ocenić spełnienie tego kryterium w odniesieniu do konkretnych kategorii produktów, usług i procesów ICT pozostają natomiast przedmiotem Krajowego Schematu Certyfikacji.

9 ICT (technologie informacyjno-komunikacyjne, ang. *Information and Communication Technology*) – branża gospodarki obejmująca przedsiębiorstwa, których głównym rodzajem działalności jest produkcja dóbr i usług pozwalających na elektroniczne rejestrowanie, przetwarzanie, transmitowanie, odtwarzanie lub wyświetlanie informacji. Źródło: GUS. Słownik pojęć. (b.d.).

Krajowy Schemat Certyfikacji Cyberbezpieczeństwa, przewidziany w art. 15 ust. 1 ustawy, jak dotąd nie został wydany. Schemat ma charakter fakultatywny, a jego brak oznacza, że system certyfikacji funkcjonuje dotąd wyłącznie na poziomie ram proceduralnych, bez konkretnej treści merytorycznej, którą mógłby wypełnić. W toku prac legislacyjnych do projektu ustawy dołączono wprawdzie projekt rozporządzenia określającego schemat „Firma Bezpieczna Cyfrowo", skierowany do sektora Małych i Średnich Przedsiębiorstw, pozostaje on jednak na etapie projektu i nie ma mocy wiążącej.

Treść przyszłego schematu nie jest jeszcze znana, jednak ustawa już dziś wyznacza dla niej punkt odniesienia. **Artykuł 7 ustawy wymaga rzeczywistego zapewnienia** m.in. **poufności i integralności przetwarzanych danych na poziomie odpowiednim do potencjalnych cyberzagrożeń oraz minimalizacji znanych ryzyk**; **tymczasem eksterytorialny, egzekwowalny dostęp organów państwa trzeciego do danych – niezależnie od miejsca ich przechowywania i bez zgody administratora – stanowi uznany wektor zagrożenia dla poufności, wobec którego środki czysto techniczne (szyfrowanie, izolacja, kontrola dostępu) pozostają z założenia nieskuteczne, ponieważ zobowiązany dostawca dysponuje także środkami umożliwiającymi odczyt danych**. Zgodnie z teorią integralności kontekstowej (Nissenbaum, 2010), naruszenie ma miejsce, gdy dane trafiają do innego odbiorcy lub zmienia się zasada, na jakiej są przekazywane – z poufnego powierzenia na pozyskanie w imię „bezpieczeństwa narodowego" – i nie musi przy tym dojść do żadnej awarii technicznej. Niepowołany odbiorca uzyskujący wgląd w dane narusza ich poufność niezależnie od tego, czy złamał zabezpieczenia.

Z tego względu **odporność na dostęp jurysdykcyjny, w tym ocena porządku prawnego, któremu podlega dostawca i jego grupa kapitałowa, jest „znanym ryzykiem w zakresie cyberzagrożeń" w rozumieniu art. 7 i mieści się w materialnym zakresie celów certyfikacji, a jej ujęcie w schemacie krajowym wydawanym na podstawie art. 15 ustawy stanowi realizację delegacji ustawowej, nie zaś jej przekro-**

czenie. Niepoprawny pogląd przeciwny opiera się bowiem na fałszywej dychotomii kwestii ,,technicznych" i ,,nietechnicznych".

Dodatkowo krajowy schemat musi pozostawać zgodny z prawem unijnym: zgodnie z Cybersecurity Act (art. 57 ust. 1 rozporządzenia 2019/881), w zakresie, w jakim dany przedmiot certyfikacji zostanie objęty europejskim programem certyfikacji cyberbezpieczeństwa, schemat krajowy musi mu ustąpić i przestaje być skuteczny z dniem wskazanym w odpowiednim akcie wykonawczym Komisji.

4.3. Ustawa chmurowa

Od 2025 r. w Ministerstwie Cyfryzacji prowadzone są prace koncepcyjne nad tzw. „Ustawą chmurową" (Ustawą o chmurze obliczeniowej), która miałaby uporządkować obecny rozproszony system regulacyjny oparty głównie na Uchwale Rady Ministrów nr 97 dotyczącej Wspólnej Infrastruktury Informatycznej Państwa (WIIP) oraz dokumencie Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). **Obecna struktura regulacyjna jest niewystarczająca zarówno z perspektywy bezpieczeństwa państwa, jak i budowy długoterminowej suwerenności cyfrowej.**

Uchwała WIIP ma charakter nienormatywny i nie może stanowić podstawy do nakładania obowiązków ustawowych. Z kolei SCCO, jako dokument wydany na podstawie uchwały, ma charakter wytycznych, a nie powszechnie obowiązującego prawa. W praktyce oznacza to, że sądy, jednostki samorządu terytorialnego oraz część podmiotów publicznych nie mają obowiązku stosowania wskazanych standardów bezpieczeństwa i zasad korzystania z chmury obliczeniowej.

Obecne regulacje nie uwzględniają w wystarczającym stopniu ryzyka wynikającego z podległości dostawców pod jurysdykcje państw trzecich. Aktualne ramy prawne nie wprowadzają również obowiązku lokalizacji danych i kluczowych usług w Europejskim Obszarze Gospodarczym ani wymagań dotyczących interoperacyjności i przenoszalności usług chmurowych. Co prawda SCCO zawiera w tym zakresie pewne wytyczne, jednak – jak wskazano powyżej – dokument ten nie ma mocy powszechnie

obowiązującego prawa i jego stosowanie pozostaje kwestią wyboru. Brak twardych wymogów prawnych zwiększa ryzyko *vendor lock-in* oraz strategicznego uzależnienia od pojedynczych dostawców spoza UE.

Co istotne z perspektywy polskich rekomendacji, CADA w Załączniku III szczegółowo określa wymagania audytowe dla każdego poziomu, obejmujące weryfikację struktury własnościowej i beneficjenta rzeczywistego dostawcy aż do ostatecznego właściciela, lokalizacji infrastruktury, personelu i danych, a także łańcucha dostaw oprogramowania. **Komisja Europejska wprost potwierdza zatem, że ocena jurysdykcji i struktury kontrolnej dostawcy jest nie tylko możliwa, ale konieczna i może być przeprowadzana przez wyspecjalizowane jednostki audytowe bez udziału służb specjalnych.**

Dla Polski oznacza to, że projektowana ustawa chmurowa oraz system certyfikacji zaufanego dostawcy powinny być budowane w bezpośredniej zgodności z poziomami zapewnienia określonymi w CADA.

4.4. System oceny krajowości

Aby wzmocnić udział lokalnych kompetencji i podmiotów (krajowych dostawców) w tworzeniu, utrzymaniu i rozwoju infrastruktury cyfrowej, Ministerstwo Aktywów Państwowych zaproponowało wykorzystanie modelu oceny krajowości.

W zależności od otrzymanej sumy wag podmiot otrzymuje ocenę krajowości w skali od 0 do 1 (0-100%):

- jednostka dominująca najwyższego szczebla (*ultimate parent unit*) znajduje się w Polsce – 25 %
- główny przedmiot działalności przedsiębiorcy jest wykonywany na terytorium Polski – 25 %
- przedsiębiorca posiada rezydencję podatkową w Polsce i odprowadza w Polsce podatek dochodowy – 15 %
- ponad 50% pracowników przedsiębiorcy posiada obywatelstwo polskie lub mieszka w Polsce oraz wykonuje pracę na terytorium

Polski i odprowadza w Polsce podatek dochodowy oraz składki na ubezpieczenia społeczne – 15 %

- przedsiębiorca posiada siedzibę w Polsce (zarejestrowaną w KRS lub CEiIDG) oraz prowadzi nieprzerwaną działalność gospodarczą na terytorium Polski od co najmniej 3 lat – 10 %
- ponad 50% rocznych obrotów przedsiębiorstwa jest generowanych na terytorium Polski – 10 %

Powyższa definicja krajowego dostawcy **pozwala zidentyfikować spółki zależne międzynarodowych korporacji technologicznych, które pomimo formalnej obecności w Polsce pozostają częścią globalnych struktur własnościowych i zarządczych**. Na znaczenie ustalenia krajowości i kontroli właścicielskiej wyraźnie zwraca też uwagę KE w projekcie rozporządzenia CADA. Model ten ma jednak charakter analityczny i nie może stanowić samodzielnego kryterium eliminacyjnego w zamówieniach publicznych.

Wprowadzenie takiej ewaluacji ma jednak istotne znaczenie dla oceny wpływu zamówień publicznych na rozwój krajowych zdolności technologicznych, nie tylko kwestię eksterytorialnej jurysdykcji czy wpływów politycznych. Pomaga ocenić, czy część generowanej wartości ekonomicznej może podlegać transferowi do podmiotów dominujących zlokalizowanych poza granicami kraju, w tym w ramach mechanizmów unikania opodatkowania i wewnątrzgrupowych przepływów finansowych. Model oceny krajowości w połączeniu z kryteriami funkcjonalnymi i oceną krytyczności infrastruktury może być stosowany wyłącznie w uzasadnionych przypadkach, takich jak bezpieczeństwo narodowe, zarządzanie danymi osobowymi obywateli, rejestrami krajowymi.

Tu warto odnotować, że w polskim porządku prawnym analiza struktury własnościowej spółek opiera się przede wszystkim na danych wynikających z Kodeksu spółek handlowych (KSH) oraz rejestrów publicznych, w szczególności Krajowego Rejestru Sądowego (KRS) i ujawnianych w nim informacji o wspólnikach, akcjonariuszach oraz strukturze organów spółki. W przypadku spółek kapitałowych możliwe

jest ustalenie formalnego rozkładu udziałów lub akcji, w tym identyfikacja podmiotów posiadających pakiety kontrolne lub znaczące pakiety mniejszościowe. KSH umożliwia analizę relacji korporacyjnych pomiędzy spółkami, w tym występowania powiązań dominacji i zależności w rozumieniu przepisów o grupach spółek oraz zasad wykonywania praw udziałowych. W określonych przypadkach możliwe jest również ustalenie struktury kontroli pośredniej, wynikającej z łańcuchów właścicielskich, choć zakres tej analizy jest ograniczony do danych ujawnianych publicznie lub możliwych do odtworzenia na podstawie dostępnych rejestrów. Punktem odniesienia do ewentualnych nowych regulacji w tym obszarze może być Francja, która w wybranych sektorach stosuje rozbudowane instrumenty kontroli inwestycji zagranicznych pozwalające na ocenę nie tylko formalną struktury właścicielskiej, lecz także faktycznej zdolności do wywierania wpływu na spółkę. W praktyce umożliwia to ograniczanie sytuacji, w których rozproszona struktura kapitałowa maskuje rzeczywiste relacje kontroli.

Jednocześnie kryterium krajowości w takim kształcie pozostaje niewystarczające dla oceny „lokalności" ponieważ nie identyfikuje przypadków pośrednictwa w sprzedaży usług oferowanych przez zagraniczne podmioty. Przykładem różnicy pomiędzy tymi koncepcjami może być **Operator Chmury Krajowej** (OChK). Spółka została powołana w 2018 roku przez PKO Bank Polski i Polski Fundusz Rozwoju jako podmiot dostarczający rozwiązania chmury obliczeniowej. OChK działa w modelu multicloud, oferując zarówno własne produkty, jak i odsprzedając usługi globalnych dostawców chmury publicznej – w tym Google Cloud i Microsoft Azure (OChK Cloud, b.d.), z którymi zawarła strategiczne partnerstwa. W praktyce oznacza to, że **polska instytucja publiczna, która korzysta z OChK w przekonaniu, iż wybiera rozwiązanie krajowe, może w rzeczywistości przetwarzać dane na infrastrukturze należącej do amerykańskich korporacji, podlegającej ich jurysdykcji i warunkom handlowym**. W konsekwencji sama struktura właścicielska przestaje być wystarczającym kryterium oceny suwerenności, jeśli nie jest uzupełniona o analizę rzeczywistej kontroli

technologicznej, architektury usług oraz powiązań z globalnymi dostawcami infrastruktury cyfrowej w całym łańcuchu. **Dla oceny faktycznej lokalności usługi lub produktu konieczne jest zatem zbadanie nie tylko krajowości bezpośredniego dostawcy, ale całego łańcucha dostaw**.

4.5 Dyskryminacja w zamówieniach publicznych

Osobnym problemem strukturalnym pozostaje prawo zamówień publicznych, które w obecnym kształcie jest narzędziem anachronicznym, niedostosowanym do specyfiki zakupów technologicznych. Ustawa konstruowana była z myślą o zamówieniach na towary, usługi remontowe czy budowlane, a dominującym kryterium wyboru pozostaje cena. Tymczasem zakup usług cyfrowych – oprogramowania, infrastruktury chmurowej, systemów krytycznych – wiąże się z szeregiem czynników pozakosztowych, takich jak jurysdykcja dostawcy, ryzyko *vendor lock-in*, koszty migracji czy bezpieczeństwo łańcucha dostaw. Obowiązujące przepisy nie dają zamawiającym skutecznych narzędzi do uwzględnienia tych kryteriów w postępowaniu, co w praktyce faworyzuje najtańszą ofertę kosztem bezpieczeństwa narodowego i suwerenności cyfrowej państwa.

Wysoki poziom uzależnienia polskiej gospodarki i instytucji publicznych od rozwiązań zagranicznych Big Techów bywa uzasadniany uczciwą konkurencją w przetargach, wyższą jakością oferowanego oprogramowania lub bardziej konkurencyjnymi cenami.

W praktyce jednak rozwiązania alternatywne wobec systemu Windows, pakietu Office czy innych produktów Microsoftu często są z góry skazane na porażkę. Jak wynika z raportu Instrat (Kopeć, 2025), w analizowanym zbiorze **99% zamówień publicznych wyklucza pośrednio lub bezpośrednio wszelką konkurencję wobec produktów oferowanych przez amerykański Big Tech**. Do wymogów w oczywisty sposób naruszających polskie prawo należą:

- wymóg, aby wszystkie funkcje w interfejsie miały takie same nazwy jak funkcje w interfejsie Microsoft;

- wymóg wsparcia VBScript, języka programowania stworzonego przez Microsoft (który jest przestarzały i sam Microsoft deklaruje, że się z niego wycofuje);
- wymóg, aby wszystkie programy były częścią tego samego pakietu (do pakietu biurowego, poza standardowymi aplikacjami do edycji tekstu, arkuszy kalkulacyjnych i prezentacji, należeć muszą również programy do zarządzania pocztą, kalendarzem lub notatnikiem z możliwością rozpoznawania tekstu pisanego ręcznie);
- wymóg, aby interfejs zawierał elementy 3D.

Wszystkie te **kryteria jawnie faworyzują dotychczasowego dostawcę, a w konsekwencji ograniczają krajowym podmiotom możliwość wzięcia udziału w uczciwym konkurowaniu w przetargach na zamówienia publiczne, co odbija się na możliwości rozwoju lokalnych kompetencji.** Tego rodzaju wymagania budzą również wątpliwości prawne, ponieważ mogą naruszać podstawowe zasady Prawa zamówień publicznych, w szczególności zasadę równego traktowania wykonawców oraz zapewnienia uczciwej konkurencji. W orzecznictwie Krajowej Izby Odwoławczej wielokrotnie podkreślano, że opis przedmiotu zamówienia nie może prowadzić do nieuzasadnionego uprzywilejowania konkretnego producenta lub technologii.

W odpowiedzi na interpelację grupy posłów (Gabriel, Jaśkowiec, Krzywonos-Strycharska, Niedźwiedzki, Siemaszko, Szopiński, Zawieja) Ministerstwo Cyfryzacji (Standerski, 2026a) stwierdza, że „**dostrzega ryzyka wynikające z nadmiernego uzależnienia jednostek sektora publicznego od rozwiązań cyfrowych tworzonych przez niewielkie grono dostawców**. Kierując się dążeniem do jego zmniejszenia, Ministerstwo Cyfryzacji wraz z Centralnym Ośrodkiem Informatyki przeprowadziło w marcu br. szerokie badanie ankietowe, na które uzyskano odpowiedzi od ponad 600 podmiotów sektora publicznego, przede wszystkim jednostek samorządu terytorialnego oraz administracji centralnej. Podstawowym celem badania było oszacowanie poziomu uzależnienia jednostek sektora publicznego od konkretnych rozwiązań cyfrowych w ramach 13 obszarów stosu technologicznego. Badano

także zainteresowanie ewentualną zmianą stosowanych rozwiązań, wykorzystanie i znajomość rozwiązań otwartoźródłowych (*open source*). Szacowano także poziom obciążenia danej jednostki wydatkami na oprogramowanie komercyjne w poszczególnych obszarach.

Wyniki badania są podstawą do prac powołanego 17 kwietnia 2026 r. **Zespołu do spraw rozwoju, upowszechniania i wsparcia wdrażania w sektorze publicznym rozwiązań typu *open source*,** który wśród zadań ma m.in. „**sformułowanie rekomendacji dla przeprowadzenia pilotażowych wdrożeń rozwiązań typu *open source* w jednostkach sektora publicznego**".

4.6. Konieczność szerszej strategii suwerennościowej

Polska stoi dziś przed koniecznością przejścia od polityki skoncentrowanej wyłącznie na cyberbezpieczeństwie do szerszej strategii suwerenności cyfrowej. Obowiązujące regulacje – od ustawy o KSC, przez ustawę o krajowym systemie certyfikacji cyberbezpieczeństwa, po wytyczne SCCO i WIIP – koncentrują się głównie na aspektach technicznych, pozostawiając bez odpowiedzi pytania o kontrolę nad danymi, zależność od dostawców spoza UE, odporność na ryzyka jurysdykcyjne oraz długoterminowe skutki gospodarcze cyfrowego uzależnienia. Tymczasem zarówno projekt unijnego rozporządzenia CADA, jak i doświadczenia innych państw, które omawiamy w dalszej części raportu, pokazują, że **bezpieczeństwo cyfrowe nie może być oddzielane od kwestii własności, kontroli i lokalizacji infrastruktury, m.in. jako warunków audytowalności czy oceny eksterytorialnej jurysdykcji oraz podatności na zewnętrzne wpływy polityczne**. Planowana ustawa chmurowa daje wyjątkową okazję do stworzenia spójnych ram prawnych, które połączą wymagania bezpieczeństwa, interoperacyjności i przenoszalności usług z aktywnym wspieraniem europejskich i krajowych dostawców technologii. Bez takich działań Polska pozostanie jedynie konsumentem zagranicznych rozwiązań cyfrowych, ponosząc rosnące koszty ekonomiczne i strategiczne związane z utratą kontroli nad kluczową infrastrukturą cyfrową.

Rozdział V
Świat w migracji do otwartych ekosystemów cyfrowych

Choć problem suwerenności cyfrowej dotyczy całej gospodarki, szczególne znaczenie ma on dla państwa i sektora publicznego. Administracja odpowiada za przetwarzanie wrażliwych danych obywateli, utrzymanie usług krytycznych oraz bezpieczeństwo państwa. Jednocześnie jako jeden z największych nabywców technologii publiczne instytucje mają istotny wpływ na rozwój rynku i poziom zależności od zagranicznych dostawców. Od kilkunastu lat rządy krajowe i lokalne prowadzą pilotażowe działania zmierzające do zwiększenia własnej kontroli nad infrastrukturą cyfrową i jej kosztami.

5.1. Wielka Brytania wychodzi z *vendor-lock-in*

W 2011 roku brytyjski rząd powołał Government Digital Service (GDS) w odpowiedzi na wieloletnie problemy związane z wysokimi kosztami (rzędu miliardów funtów rocznie) oraz niską efektywnością systemów informatycznych w administracji publicznej. Wcześniej państwo wydawało znaczące środki publiczne na projekty realizowane przez prywatne firmy IT, które często charakteryzowały się niskim poziomem interoperacyjności, trudnościami w utrzymaniu oraz silnym uzależnieniem instytucji publicznych od pojedynczych dostawców technologii. **Celem GDS było stworzenie wspólnych standardów cyfrowych oraz zwiększenie wewnętrznych kompetencji administracji w zakresie projektowania i zarządzania systemami IT, przy jednoczesnym ograniczeniu zależności od dużych korporacji technologicznych.**

Jednym z kluczowych narzędzi wdrożonych przez GDS był program G-Cloud oraz powiązana z nim platforma Digital Marketplace. Reforma ta zmieniła model zakupów usług cyfrowych i chmurowych w admini-

stracji publicznej. Zamiast wieloletnich, zamkniętych kontraktów realizowanych przez kilku dominujących integratorów IT, państwo stworzyło otwarty rynek usług cyfrowych, do którego mogły dołączać również małe i średnie firmy technologiczne. Urzędy uzyskały możliwość szybkiego porównywania ofert różnych dostawców oraz kupowania konkretnych usług chmurowych, takich jak hosting, przechowywanie danych czy oprogramowanie SaaS, bez konieczności organizowania kosztownych i wielomiesięcznych przetargów (Kattel i in., 2023).

Kluczowym elementem reformy było potraktowanie interoperacyjności, otwartych standardów i innych metod unikania *vendor lock-in* jako formalnych kryteriów polityki zakupowej państwa i dzięki temu zwiększania suwerenności cyfrowej. Kontrakty zostały podzielone na mniejsze moduły, co ograniczyło przewagę największych korporacji technologicznych i umożliwiło lokalnym firmom realne konkurowanie o zamówienia publiczne. Dzięki standaryzacji wymagań oraz uproszczeniu procedur administracyjnych brytyjski sektor publiczny zaczął stopniowo budować bardziej zróżnicowany ekosystem dostawców usług cyfrowych.

5.2. Kraje UE na drodze do suwerenności

5.2.1. Francuska żandarmeria buduje własne Ubuntu

W 2005 roku, w związku z zapowiedziami stopniowego wygaszania wsparcia i rozwoju systemu Windows XP przez Microsoft oraz planowanym przejściem na jego następcę, **francuska żandarmeria wojskowa rozpoczęła proces stopniowej migracji z rozwiązań Microsoftu, argumentując to wysokimi kosztami modernizacji oraz uzależnieniem od jednego dostawcy.** Zmiana oprogramowania na Windows Vista wymagałaby bowiem wykupienia nowych licencji oraz nowego sprzętu z powodu wyższych wymagań sprzętowych.

W pierwszym etapie wdrożono narzędzia oparte na wolnym oprogramowaniu, takie jak pakiet biurowy OpenOffice, przeglądarka Firefox i klient poczty Thunderbird. Następnie w 2008 roku stworzono GendBuntu – własną dystrybucję systemu operacyjnego Ubuntu, który rozwijany był od 2004 r. jako wolne oprogramowanie na licencji *copyleft*. Proces migracji realizowano etapami przez kolejne lata, obejmując nim stopniowo dziesiątki tysięcy stanowisk pracy, a jego zasadnicze sfinalizowanie nastąpiło około 2014 roku (Draouil, 2025).

Według dostępnych danych rozwiązanie to przyniosło oszczędności rzędu około 2 mln euro rocznie w kosztach licencyjnych (Canonical Ubuntu, 2010) oraz pozwoliło ograniczyć konieczność wymiany sprzętu dzięki niższym wymaganiom systemowym. Architektura oparta na Linuxie pozwoliła na zmniejszenie liczby inwazyjnych aktualizacji.

5.2.2. Szlezwik-Holsztyn przechodzi na FOSS

W 2025 roku rząd kraju związkowego Szlezwik-Holsztyn ogłosił decyzję o odejściu od Microsoft Exchange i Outlooka na rzecz rozwiązań *open source*: Open-Xchange oraz Thunderbird (Vaughan-Nichols, 2025). **Decyzję uzasadniono potrzebą ograniczenia zależności ekonomicznej i technologicznej oraz zwiększenia kontroli nad przetwarzaniem danych**, w tym wrażliwych, w administracji publicznej, i szerzej, nad procesami ICT. **Migracja obejmie 30 tysięcy urzędników.**

5.2.3. Dania stawia na *copyleft*

W tym samym roku duńskie ministerstwo spraw zagranicznych zapowiedziało migrację z Microsoft 365 na LibreOffice (pakiet biurowy oparty o wolne oprogramowanie i *copyleft*) (Sneddon, 2025). Równolegle decyzje o odejściu od ekosystemu Microsoftu ogłosiły również Kopenhaga i Aarhus. **W debacie publicznej wskazywano m.in. na rosnące ryzyka geopolityczne oraz kwestie bezpieczeństwa danych w kontekście m.in. kwestii Grenlandii oraz obaw o potencjalne szpiegostwo** (Desmarais, 2025)**.**

5.2.4. Francja wdraża plan na odzyskanie suwerenności cyfrowej: 2,5 mln urzędników przejdzie na Linux

W kwietniu 2026 roku francuska Międzyresortowa Dyrekcja ds. Cyfryzacji (DINUM) ogłosiła rozpoczęcie największej w historii Europy migracji administracji publicznej z systemu operacyjnego Windows na Linux. Celem przedsięwzięcia jest ograniczenie niezależności państwa od amerykańskich technologii i wzmocnienie suwerenności cyfrowej. Do jesieni 2026 roku wszystkie ministerstwa mają przedstawić szczegółowe plany transformacji struktur IT. Docelowo migracja ma objąć 2,5 mln urzędników państwowych, z czego 500 tys. ma przejść na Linux do końca 2027 roku („France swaps Windows…", 2026). Według dostępnych informacji, jeszcze w maju 2026 roku nowe rozwiązania zostały wdrożone dla 80 tys. pracowników publicznej służby zdrowia.

Reforma wpisuje się we francuską strategię cyfrową, o której mówił Emmanuel Macron podczas European Digital Sovereignty Summit w 2025 roku (Élysée, 2025; DWS News, 2025). **W swoim wystąpieniu Prezydent Macron podkreślał, że Europa nie może stać się technologicznym wasalem Stanów Zjednoczonych ani Chin. Zwracał również uwagę na konieczność odejścia od modelu, w którym europejskie państwa pełnią jedynie rolę klientów zagranicznych Big Techów, zamiast rozwijać własne technologie.** Według francuskiego prezydenta **kluczowe znaczenie mają większe inwestycje w innowacje, badania oraz rozwój** nowoczesnych technologii, ponieważ to właśnie one mają stanowić fundament europejskiej konkurencyjności. **Zapowiedział także zwiększenie inwestycji w europejską infrastrukturę tzw. sztucznej inteligencji, obejmującą budowę centrów danych, rozwój europejskich modeli AI oraz zwiększanie mocy obliczeniowej dostępnej na terenie Unii Europejskiej.** Istotnym elementem strategii ma być również zasada *local content*, zakładająca preferowanie europejskich dostawców w zamówieniach publicznych. Francuski prezydent podkreślał ponadto potrzebę **szerszego wykorzystania FOSS jako sposobu na zwiększenie niezależności technologicznej**.

Osiąganie tych celów jest możliwe **dzięki wspieraniu lokalnych dostawców infrastruktury i chmury poprzez rygorystyczny system kwalifikacji usług chmurowych**. W 2016 r. francuska agencja ds. cyberbezpieczeństwa (ANSSI) opracowała SecNumCloud – zbiór wymagań bezpieczeństwa, organizacyjnych i prawnych dla usług chmurowych. Na jego podstawie ANSSI prowadzi proces kwalifikacji, w ramach którego oceniane są konkretne usługi chmurowe. Aby uzyskać kwalifikację SecNumCloud, **dostawca musi spełnić szereg warunków**, **m.in.**:

- **kontrola operacyjna nad infrastrukturą i danymi** musi być **na terytorium Unii Europejskiej**,
- ograniczenie wpływu podmiotów spoza UE na zarządzanie usługą, a także zapewnienie, że operacyjne zarządzanie systemem odbywa się przez **personel podlegający europejskiej jurysdykcji**,
- **odporność na dostęp administracyjny wynikający z przepisów państw trzecich**.

Choć formalnie nie promuje on konkretnych firm krajowych, jego wymagania sprawiają, że na rynku powstają rozwiązania „zaufanej chmury" kontrolowane przez podmioty europejskie, czasem w modelach partnerskich z globalnymi dostawcami technologii.

> ***Sovereignty washing*** to praktyka polegająca na marketingowym lub regulacyjnym **przedstawianiu usług cyfrowych, infrastruktury lub modeli chmurowych jako „suwerennych", „europejskich" lub „krajowych", mimo że w rzeczywistości kluczowe elementy kontroli technologicznej, operacyjnej lub prawnej pozostają zależne od podmiotów spoza danej jurysdykcji**. Najczęściej zarzut washingu pojawia się wobec ofert określanych jako „*sovereign cloud*" lub „*EU sovereign cloud*", które formalnie spełniają część wymogów (np. lokalizacja danych w Europie), ale zdaniem krytyków nie rozwiązują problemu zależności od zagranicznego dostawcy technologii,

jurysdykcji lub kontroli nad oprogramowaniem (L'Echo, b.d.). Najbardziej oczywistym przykładem są europejskie inicjatywy hiperskalerów: Microsoft Sovereign Cloud, AWS European Sovereign Cloud oraz analogiczne rozwiązania Google Cloud. Krytycy wskazują, że choć dane mogą być przechowywane i przetwarzane w Europie, to spółki pozostają amerykańskie i nadal podlegają amerykańskim regulacjom, takim jak CLOUD Act czy FISA 702. Drugim często przywoływanym przypadkiem jest Delos Cloud w Niemczech, spółka zależna SAP rozwijana na potrzeby administracji publicznej. Choć przedstawiana jest jako rozwiązanie suwerenne, opiera się na technologii Microsoftu i wymaga ciągłego dostępu do aktualizacji oraz rozwoju oprogramowania kontrolowanego przez pozaeuropejskiego dostawcę (Brecht, 2024).

Podobne kontrowersje pojawiają się wokół francuskich projektów S3NS (Thales + Google Cloud) oraz Bleu (Capgemini/Orange + Microsoft) (Piquard, 2025). Zwolennicy argumentują, że dzięki lokalnej kontroli operacyjnej, europejskiemu personelowi, odrębnej infrastrukturze i zarządzaniu kluczami kryptograficznymi spełniają one wymagania suwerenności. Krytycy odpowiadają jednak, że kluczowe komponenty technologiczne, rozwój platformy oraz część zależności pozostają pod kontrolą amerykańskich dostawców, dlatego określają te rozwiązania mianem *sovereignty washing* lub „suwerenności przez franczyzę".

Dowodem na zmianę w podejściu jest decyzja dotycząca Health Data Hub, czyli centralnej platformy danych zdrowotnych. Po wieloletniej debacie dotyczącej wykorzystania Microsoft Azure francuskie Ministerstwo Zdrowia zdecydowało w 2026 r. o wyborze krajowego dostawcy – Scaleway.

W 2026 r. organizacja CISPE zrzeszająca europejskich dostawców chmurowych ostrzegła Komisję Europejską przed zjawiskiem *sovereignty washing* i argumentowała, że część

ofert reklamowanych jako „europejskie" lub „suwerenne" nie spełnia wymogów faktycznej niezależności od podmiotów spoza UE („Joint Call for a Sovereign and Resilient European Cloud Policy", 2026).

Zarzut *sovereignty washing* pokazuje przesunięcie debaty. Jeszcze kilka lat temu za wystarczające uznawano przechowywanie danych w Europie. Obecnie podnosi się, że **rzeczywista suwerenność wymaga również kontroli m.in. nad kluczami kryptograficznymi, personelem, procesem aktualizacji oprogramowania, telemetrią, podwykonawcami** oraz rozwojem technologii.

5.2.5. Monachium: wyzwania migracji

W 2003 roku władze Monachium zdecydowały o rozpoczęciu procesu odejścia od systemów Microsoftu i migracji całej administracji na rozwiązania *open source*. Decyzja była związana z kończącym się wsparciem dla Windows NT, a także rosnącymi kosztami licencji oraz modernizacji. W ramach programu LiMux rozpoczęto stopniowe wdrażanie systemu operacyjnego opartego na Linuxie oraz pakietów biurowych FOSS, co objęło dziesiątki tysięcy stanowisk urzędniczych i wymagało równoległego stworzenia oraz dostosowania szeregu narzędzi administracyjnych do potrzeb lokalnej administracji (Thoma, 2017).

Przejście na LiMux pozwoliło miastu ograniczyć wydatki licencyjne oraz częściowo uniknąć kosztów związanych z cyklicznymi przymusowymi modernizacjami sprzętu, wynikającymi z wymogów kolejnych wersji oprogramowania Microsoftu. Według danych przedstawianych przez władze Monachium **całkowite oszczędności projektu mogły sięgnąć około 10 milionów euro.** Jednocześnie zwiększono kontrolę nad infrastrukturą IT oraz ograniczono zależność od jednego, zagranicznego dostawcy oprogramowania. Mimo to w 2017 władze miasta zdecydowały o powrocie administracji do Windows (Adach, 2024).

Jednym z istotnych wyzwań wdrożenia była interoperacyjność z systemami zewnętrznymi. Część stanowisk musiała pozostać przy systemie Windows ze względu na konieczność komunikacji z administracją federalną oraz instytucjami Unii Europejskiej. Jednak w 2026 władze Monachium postanowiły wznowić projekt, argumentując to potrzebą tworzenia suwerenności cyfrowej i ograniczeniem zależności od jednego dostawcy. Wskazuje to, że mimo trudności z migracją władze są świadome potrzeby podejmowania stanowczych działań.

Z perspektywy Polski doświadczenia Monachium wskazują, że kluczowe znaczenie ma nie tyle jednorazowa, całościowa wymiana środowiska informatycznego, ile stopniowe etapowanie migracji oraz konsekwentne budowanie zdolności wyjścia (*exit capability*) poprzez wykorzystanie otwartych standardów i interoperacyjnych rozwiązań. Celem polityki cyfrowej powinno być zapewnienie administracji możliwości zmiany dostawcy bez ponoszenia nadmiernych kosztów i ryzyka operacyjnego.

5.3. Przetarg KE na suwerenną chmurę

W październiku 2025 r. Komisja Europejska uruchomiła pierwszy przetarg na suwerenne usługi chmurowe dla instytucji Unii Europejskiej w ramach systemu zakupowego Cloud III Dynamic Purchasing System, o wartości do 180 mln euro na okres sześciu lat. Celem przetargu było wzmocnienie pozycji unijnych instytucji, organów, urzędów i agencji. Dodatkowym założeniem było zachęcenie rynku do oferowania suwerennych rozwiązań cyfrowych zgodnych z prawem i wartościami UE.

Podstawą oceny ofert był opracowany przez Komisję ***Cloud Sovereignty Framework* 1.2.1, który po raz pierwszy w historii europejskich zamówień publicznych przełożył abstrakcyjne pojęcie suwerenności na obiektywne, audytowalne i porównywalne kryteria oceny** – przed jego opracowaniem nie było technicznie możliwe egzekwowanie suwerenności jako wymogu przetargowego.

17 kwietnia 2026 r. Komisja ogłosiła rozstrzygnięcie przetargu, przyznając cztery równoległe kontrakty europejskim firmom. Były to: luksembursko-francuskie konsorcjum Post Telecom z OVHCloud i CleverCloud, niemiecka spółka StackIT, francuska Scaleway oraz belgijsko-francusko-luksemburskie konsorcjum Proximus, Clarence i Mistral. Komisja świadomie wybrała model czterech dostawców zamiast jednego, aby zapewnić dywersyfikację i odporność na ryzyko uzależnienia od jednego podmiotu. Post Telecom, StackIT i Scaleway osiągnęły poziom SEAL-3, czyli pełną odporność cyfrową, natomiast Proximus uzyskał poziom SEAL-2, z powodu korzystania z usług S3NS – spółki joint venture Thales i Google Cloud. Poziom SEAL-2 stanowił minimalny wymóg kwalifikacyjny w przetargu.

Włączenie do grona zwycięzców konsorcjum Proximus, opartego częściowo na platformie Google Cloud, wywołało debatę w europejskim sektorze technologicznym. Komisja odniosła się do tego wprost, stwierdzając, że technologie spoza Europy mogą spełniać minimalny wymóg suwerennościowy (SEAL-2) pod warunkiem, że są zarządzane w ramach rygorystycznych i odpowiednich struktur nadzoru europejskiego (Komisja Europejska, 2026).

Rozstrzygnięcie przetargu ma znaczenie wykraczające poza samą Komisję. Zachęca ono wszystkie organizacje, zarówno publiczne, jak i prywatne, do korzystania z *Cloud Sovereignty Framework* w celu wzmocnienia własnej suwerenności cyfrowej i odporności. Skala zainteresowania okazała się na tyle duża, że 1 czerwca 2026 r. Komisja opublikowała dodatkowe wyjaśnienia dotyczące zawartości Frameworku wraz ze szczegółową dokumentacją 48 kryteriów oceny, pogrupowanych w osiem kategorii suwerennościowych, oraz metodologią obliczania Sovereignty Score.

Prawdziwym przełomem jest jednak sam fakt, że **suwerenność cyfrowa po raz pierwszy stała się formalnym kryterium wyboru dostawcy usług publicznych – na równi z ceną i parametrami technicznymi.** Oznacza to zmianę paradygmatu: bezpieczeństwo cyfrowe i suwerenność przestają być postulatami politycznymi, a stają się mie-

rzalnymi wymaganiami zamawiającego. Dla administracji publicznych w całej Europie, w tym w Polsce, jest to sygnał, że pytanie nie brzmi już „czy" uwzględniać kryteria suwerennościowe w zamówieniach na usługi cyfrowe, lecz „kiedy" i „jak".

5.4. Stany Zjednoczone przejmują TikTok

W sierpniu 2020 r. administracja Donalda Trumpa wydała rozporządzenie wykonawcze (Executive Order 13942), argumentując, że **podleganie ByteDance prawu chińskiemu potencjalnie umożliwia temu państwu dostęp do danych użytkowniczek i użytkowników, a sama platforma TikTok może wpływać na obieg informacji w Stanach Zjednoczonych**. Rozporządzenie to zostało jednak zablokowane przez sądy federalne, a w czerwcu 2021 r. formalnie uchylone przez administrację Joe Bidena, która zastąpiła je odrębnym mechanizmem przeglądu bezpieczeństwa. Właściwą podstawą prawną stała się dopiero ustawa Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA), podpisana przez prezydenta Bidena w kwietniu 2024 r. przy szerokim, ponadpartyjnym poparciu Kongresu. Jej logika zakładała, że **dalsze funkcjonowanie TikToka w USA będzie możliwe jedynie pod warunkiem zmiany struktury kontroli właścicielskiej nad platformą poprzez zbycie jej części na rzecz podmiotów amerykańskich.** W przeciwnym razie aplikacja mogłaby zostać wyłączona z dystrybucji oraz aktualizacji na rynku amerykańskim (Tewari, 2026).

17 stycznia 2025 r. Sąd Najwyższy USA jednogłośnie odrzucił odwołanie TikToka, dając ByteDance czas do 19 stycznia 2025 r. na zbycie spółki pod groźbą wyłączenia z amerykańskiego rynku (mechanizm takiego „wyłączenia" polegał m.in. na tym, że sklepy takie jak Apple App Store czy Google Play nie mogłyby już udostępniać TikToka do pobrania). Gdy termin ten faktycznie minął, aplikacja na kilka godzin przestała działać w USA – jednak Donald Trump, obejmując urząd 20 stycznia 2025 r., wstrzymał egzekwowanie ustawy i wielokrotnie przesuwał termin sprzedaży. 25 września 2025 r. ostatecznie podpisał roz-

porządzenie uznające zaproponowaną strukturę zbycia za spełniającą wymogi prawne. Nowa, amerykańska spółka joint venture miała przejąć działalność TikToka w USA, z udziałem ByteDance ograniczonym poniżej 20%, a danymi użytkowników przechowywanymi w amerykańskiej infrastrukturze chmurowej. **Transakcja odbyła się w styczniu 2026, a kontrola w nowej spółce USDS Joint Venture LLC znalazła się w rękach konsorcjum inwestorów amerykańskich i sojuszniczych, wśród których główną rolę odgrywały Oracle, Silver Lake i MGX (Levin, 2026).**

Mechanizm ten nie stanowił klasycznego wywłaszczenia, lecz warunkowanie dostępu do rynku krajowego spełnieniem określonych wymogów bezpieczeństwa. W tym sensie przypadek TikToka można interpretować jako przykład suwerenności jurysdykcyjnej państwa stosowanej wobec globalnej platformy cyfrowej w sytuacji, gdy kontrola nad przepływem danych, algorytmami rekomendacji oraz infrastrukturą komunikacyjną została uznana za element bezpieczeństwa narodowego. Pokazuje to, że w sytuacjach strategicznych władze mogą traktować infrastrukturę cyfrową jako obszar regulacji bezpieczeństwa, a **państwa, nawet promujące od lat model liberalny, mogą stosować instrumenty ograniczające swobodę działania globalnych platform cyfrowych kosztem klasycznych zasad wolnego rynku**. Co warto podkreślić, polityka ta była konsekwentnie realizowana niezależnie od zmieniającej się administracji USA.

Należy jednak zastrzec, że amerykański mechanizm warunkuje dostęp do rynku krajowego spełnieniem określonych wymogów, a jego konstrukcja prawna – oparta na specyficznej dla USA architekturze uprawnień prezydenckich w zakresie bezpieczeństwa narodowego oraz na orzecznictwie sądów amerykańskich – nie ma bezpośredniego odpowiednika w systemie UE.

Przedstawione przypadki pokazują, że **suwerenność cyfrowa staje się jednym z kluczowych elementów współczesnego bezpieczeństwa** państwa, a **konsekwentnie wprowadzana polityka suwerennościowa może doprowadzić w krótkim czasie do oszczędności oraz do ograniczenia zależnośc**i od zewnętrznych dostawców technologii.

Rozdział VI
Fundamenty suwerenności cyfrowej

Skuteczna transformacja cyfrowa państwa powinna opierać się na kilku filarach, które omawiamy poniżej.

6.1. Interoperacyjność i otwartość

Interoperacyjność powinna zostać uznana za fundamentalny standard projektowy systemów informatycznych administracji publicznej, stanowiący warunek konieczny dla realizacji celów suwerenności cyfrowej. Oznacza to systemowe odejście od architektur zamkniętych na rzecz rozwiązań opartych na otwartych standardach, umożliwiających wymianę danych i usług w sposób niezależny od konkretnego dostawcy technologii.

Kluczowe znaczenie ma zapewnienie interoperacyjności systemów (w tym poprzez **stosowanie otwartych standardów i API, ocenę przenoszalności i *exit capability***), ponieważ umożliwia ona współpracę różnych rozwiązań i zapobiega tworzeniu zamkniętych ekosystemów technologicznych. Państwo zachowuje wówczas możliwość podejmowania najkorzystniejszych decyzji w obszarze ICT i szybkiego reagowania na zmieniający się kontekst technologiczny, gospodarczy czy geopolityczny.

Istotne jest, aby wymóg interoperacyjności był egzekwowany de facto, a nie wyłącznie de jure. Meta, implementując interoperacyjność komunikatorów WhatsApp i Messenger w ramach Digital Markets Act, zaprojektowała ją w sposób oparty na kontrolowanych interfejsach API, NDA i mechanizmach centralnie zarządzanych przez Meta, a nie na otwartych standardach federacyjnych. W praktyce oznacza to, że podmioty trzecie muszą uzyskać dostęp do środowiska Meta na warunkach ustalanych jednostronnie przez Big Tech. Poprzez wymóg dostępu do takich danych i mechanizmów, jak np. identyfikacja en-

dpointów, metadanych połączeń i parametrów routingu, w praktyce Meta uniemożliwia połączenie z architekturą federacyjną Fediverse/Mastodona (Meijer, 2025).

6.2. FOSS i *copyleft*

Istotne jest wykorzystanie rozwiązań FOSS, które zwiększają przejrzystość systemów, dają administracji, ale i społeczeństwu, większą kontrolę nad infrastrukturą cyfrową, w tym możliwość rozwoju własnych rozwiązań, dopasowanych do potrzeb danej instytucji. Z tego powodu **wszystkie państwa europejskie starające się odzyskać suwerenność cyfrową aktywnie wspierają FOSS**.

Znaczenie ma również aspekt ekonomiczny, choć nie jest to bezwarunkowe. Całkowity koszt posiadania (TCO) i eksploatacji systemu obejmuje bowiem nie tylko opłaty licencyjne, lecz także koszty wdrożenia, migracji, integracji, utrzymania, wsparcia technicznego oraz szkoleń. Ostateczny bilans zależy więc od skali działania i kompetencji danej organizacji. Mimo to **w perspektywie długoterminowej rozwiązania FOSS często pozwalają ograniczyć wydatki związane z licencjami, zmniejszyć ryzyko uzależnienia od jednego dostawcy oraz wspierać rozwój *local content*, tworząc miejsca pracy i wzmacniając krajowe kompetencje technologiczne**.

Dzięki możliwości audytu, modyfikacji i współdzielenia kodu, FOSS wzmacniają przejrzystość, interoperacyjność oraz zdolność państwa do samodzielnego utrzymywania i rozwijania infrastruktury cyfrowej, stanowiąc jeden z fundamentów długoterminowej suwerenności technologicznej. Należy przy tym zwracać uwagę na różnicę między dostępnością kodu, rozumianą wyłącznie jako możliwość wglądu w kod, a wolnym i otwartym oprogramowaniem, które dzięki odpowiednim licencjom gwarantuje użytkownikom prawo do analizowania, modyfikowania i rozpowszechniania kodu.

W połączeniu z licencjami typu *copyleft* FOSS jest nie tylko rozwiązaniem technicznym, lecz także narzędziem polityki rozwojowej.

Pozwala **zatrzymać większą część wartości ekonomicznej w lokalnej gospodarce, wspiera rozwój krajowych kompetencji technologicznych** i dóbr wspólnych, a jednocześnie ogranicza przejmowanie efektów wypracowanych ze środków publicznych przez globalnych monopolistów.

6.3. Rozwój krajowych kompetencji i badanie lokalności

Rozwój krajowych kompetencji oraz wzmacnianie lokalnego łańcucha wartości stanowią istotny element budowy suwerenności cyfrowej. Obejmuje to zdolność krajowych podmiotów do projektowania, wdrażania, utrzymania i rozwijania infrastruktury cyfrowej, a także udział lokalnych firm, specjalistów i instytucji badawczych m.in. w realizacji zamówień publicznych. Takie podejście sprzyja akumulacji wiedzy i kompetencji w gospodarce, zwiększa odporność na zewnętrzne zakłócenia oraz ogranicza zależność od pojedynczych zagranicznych dostawców.

Jednocześnie, jak wskazaliśmy powyżej, **brak jest dziś mechanizmu badania lokalności i wzmacniania rozwoju lokalnych dostawców** czy to w zamówieniach publicznych, czy poprzez inne mechanizmy. Model oceny krajowości dostawców uwzględnia m.in. strukturę własności, lokalizację działalności, rezydencję podatkową, strukturę zatrudnienia, siedzibę oraz udział przychodów generowanych w kraju. Jednak **sama formalna ocena krajowości jest niewystarczająca do oceny faktycznej lokalności dostawcy**, ponieważ nie obejmuje identyfikacji wszystkich dostawców w łańcuchu wartości – co ilustruje wspomniany przykład Operatora Chmury Krajowej, który mimo krajowej struktury właścicielskiej działa w oparciu o usługi hiperskalerów. **W konsekwencji ocena suwerenności wymaga analizy nie tylko bezpośredniego dostawcy, lecz całego łańcucha technologicznego i powiązań z globalną infrastrukturą cyfrową**. Tego typu rozwiązania, tzn. **badanie łańcucha dostaw, w pewnym stopniu przewiduje dyrektywa NIS2,** jeśli chodzi o badanie poziomu bezpieczeństwa.

Pamiętać przy tym należy, że konieczne jest projektowanie instrumentów wsparcia w sposób, który będzie zgodny z zasadami jednolitego

rynku Unii Europejskiej, w szczególności zasadą równego traktowania wykonawców i niedyskryminacji. Oznacza to, że należy stosować takie kryteria zamówień publicznych, które promują suwerenność cyfrową poprzez wymagania funkcjonalne, jurysdykcyjne, środowiskowe itp., a nie poprzez bezpośrednie preferencje o charakterze narodowym.

6.4. Ochrona przed naruszeniami wynikającymi z eksterytorialnych jurysdykcji

Ochrona przed eksterytorialnymi jurysdykcjami jest kluczowa dla zachowania realnej kontroli państwa nad danymi, infrastrukturą i procesami decyzyjnymi. **Ryzyko dostępu organów państw trzecich do danych publicznych oraz wpływu na działanie systemów cyfrowych osłabia suwerenność operacyjną i prawną**. Ograniczanie tego ryzyka wymaga stosowania rozwiązań lokalizujących przetwarzanie danych w EOG, preferowania (a na wyższych poziomach krytyczności – wymogu) dostawców podlegających europejskiej jurysdykcji, wprowadzania oceny kontroli właścicielskiej i łańcucha dostaw oraz ryzyka prawnego w zamówieniach publicznych. Istotne jest przy tym badanie zasięgu jurysdykcji we wszystkich warstwach infrastruktury, w tym wspomniane już wcześniej kwestie takie, jak kontrola kluczy po stronie podmiotu europejskiego, ograniczenie dostępu personelu spoza EOG, audytowalność i odporność operacyjna.

6.5. Informacja to podstawa: audyt wewnętrzny, dane publiczne

Państwo powinno aktywnie badać swój poziom uzależnienia, jednocześnie dbając, by taki audyt mogli przeprowadzać niezależnie badaczki i badacze akademiccy i ze społeczeństwa obywatelskiego. Obecnie brakuje podstawowych danych na ten temat. Dlatego postulujemy przeprowadzenie audytu wewnętrznego w instytucjach publicznych w celu wyliczenia kosztów, jakie ponosi nasze państwo na rzecz rozwiązań konkretnych firm (w tym Big Techów) i udostępnienia tych

informacji opinii publicznej. Audyt powinien objąć całość wydatków cyfrowych, w szczególności licencje na oprogramowanie biurowe, systemowe i specjalistyczne, opłaty za usługi chmurowe i infrastrukturę obliczeniową, koszty subskrypcji platform i narzędzi SaaS, a także wydatki na integrację i utrzymanie systemów opartych na zagranicznych rozwiązaniach. Tylko pełny obraz tych kosztów (zawierający kwoty, ale też nazwy dostawców), często rozproszonych między dziesiątki instytucji i ukrytych w budżetach operacyjnych, pozwoli na świadomą debatę o skali uzależnienia i realnych korzyściach z rozwijania krajowych rozwiązań.

Wiesław Wilk

Przewodniczący Związku Pracodawców – Polska Chmura

fot. Mateusz Lelek

Przez lata dyskutowaliśmy o tym, kto dostarczy państwu technologię. Zdecydowanie rzadziej zadawaliśmy sobie pytanie, od kogo państwo będzie zależne za pięć czy dziesięć lat. To właśnie od odpowiedzi na to pytanie zaczyna się dziś rozmowa o suwerenności cyfrowej. Nie chodzi bowiem o wybór konkretnego dostawcy czy technologii, ale o zdolność państwa do zachowania kontroli nad infrastrukturą, danymi i procesami, od których zależy jego funkcjonowanie.

Dlatego za jedną z najważniejszych rekomendacji raportu uważam postulat przeprowadzenia kompleksowego audytu zależności technologicznych administracji publicznej. W Polsce wciąż nie dysponujemy pełnym obrazem tego, komu powierzamy strategiczne dane, od jakich technologii jesteśmy uzależnieni ani jakie byłyby konsekwencje utraty dostępu do kluczowych usług cyfrowych. Trudno budować skuteczną politykę bezpieczeństwa bez takiej wiedzy. Najpierw trzeba zdiagnozować skalę zależności, a dopiero później projektować mechanizmy ich ograniczania.

Równie istotne jest odejście od myślenia, że bezpieczeństwo infrastruktury można oceniać wyłącznie przez pryzmat lokalizacji danych. Serwer stojący w Polsce nie oznacza automatycznie, że państwo zachowuje nad nimi kontrolę. O rzeczywistym poziomie bezpieczeństwa decyduje również jurysdykcja, której podlega dostawca, możliwość wywierania wpływu przez organy państw trzecich czy zdolność zapewnienia ciągłości działania w sytuacji kryzysowej. Wybierając rozwiązania technologiczne, wybieramy jednocześnie określony porządek prawny i model odpowiedzialności za dane.

To samo wyzwanie zaczyna dotyczyć sztucznej inteligencji. Jeżeli modele AI będą coraz szerzej wykorzystywane w administracji publicznej, ochronie zdrowia czy sektorze finansowym, pytania o jurysdykcję, kontrolę nad danymi treningowymi, możliwość audytu modeli czy ich dalszego rozwoju staną się równie ważne jak dziś pytania dotyczące

infrastruktury chmurowej. Suwerenność cyfrowa nie kończy się na centrach danych – obejmuje cały ekosystem technologiczny, który będzie decydował o konkurencyjności gospodarki i sprawności państwa.

Na tym tle szczególnie interesująca wydaje się zawarta w raporcie rekomendacja testu suwerenności. Jego największą wartością nie jest sam model oceny czy system kaskadowy, ale próba odpowiedzi na pytanie, którego administracja publiczna do tej pory praktycznie sobie nie zadawała: jak mierzyć ryzyko uzależnienia technologicznego? Dziś przy zakupie usług dostępu do infrastruktury cyfrowej analizujemy przede wszystkim cenę, funkcjonalność czy zgodność z wymaganiami technicznymi. Znacznie rzadziej oceniamy długoterminowe skutki wyboru konkretnego rozwiązania – możliwość migracji, ryzyko *vendor lock-in*, zależność od pojedynczego dostawcy czy wpływ decyzji zakupowych na rozwój krajowych kompetencji.

Nieprzypadkowo podobne dyskusje prowadzone są dziś w wielu krajach Europy. Francja rozwija własny model zaufanej chmury, Niemcy i Dania wzmacniają wymagania dotyczące infrastruktury publicznej, a Komisja Europejska coraz wyraźniej akcentuje potrzebę budowania europejskich kompetencji cyfrowych. Nie wynika to z chęci ograniczania konkurencji ani odrzucania globalnych technologii. To efekt uznania infrastruktury cyfrowej za element bezpieczeństwa państwa i odporności gospodarki.

Warto przy tym pamiętać, że suwerenność cyfrowa nie oznacza budowania cyfrowych granic. Otwarty rynek pozostaje fundamentem rozwoju innowacji. Jednocześnie państwo ma prawo i obowiązek określać wymagania wobec technologii wykorzystywanych w obszarach o znaczeniu strategicznym. Tak samo jak definiujemy standardy dla infrastruktury energetycznej czy telekomunikacyjnej, tak też powinniśmy określać zasady dotyczące infrastruktury cyfrowej, która staje się dziś jednym z najważniejszych zasobów państwa.

Największym ryzykiem nie jest to, że Polska wybierze niewłaściwy model suwerenności cyfrowej. Największym ryzykiem jest to, że nie stworzy żadnego modelu i nadal będzie podejmować strategiczne decyzje technologiczne głównie w oparciu o cenę oraz krótkoterminową wygodę. W świecie, w którym infrastruktura cyfrowa staje się jednym z filarów bezpieczeństwa państwa, taki sposób myślenia przestaje być wystarczający.

Rozdział VII
Rozwiązania

7.1. Test suwerenności

Test suwerenności to instrument zapowiedziany przez premiera Donalda Tuska podczas Europejskiego Kongresu Finansowego w czerwcu 2026 roku, który miałby być **stosowany przy zakupach technologicznych na potrzeby państwa powyżej 5 mln zł lub 15 mln zł** w przypadku inwestycji infrastrukturalnych, pozwalając zbadać, na ile dany projekt pozostawia państwu polskiemu kontrolę nad własnymi systemami i danymi. **Rekomendujemy, aby instrument ten uzyskał podstawę ustawową** i był stosowany podczas zakupu infrastruktury cyfrowej. **Jednocześnie proponujemy inną logikę – zamiast podejścia wyłącznie kwotowego, ocenę infrastruktury pod kątem jej krytyczności.**

Projektując test, należy pamiętać, że samo kryterium fizycznej lokalizacji infrastruktury na terytorium Europejskiego Obszaru Gospodarczego ma charakter niewystarczający z perspektywy zapewnienia realnej suwerenności danych. Dane przetwarzane na serwerach zlokalizowanych w Polsce, lecz pozostających pod kontrolą podmiotu podlegającego jurysdykcji państw trzecich, nie mogą być uznane za w pełni bezpieczne, ponieważ mogą podlegać obowiązkom ujawnienia wobec organów obcych państw na mocy przepisów obowiązujących w państwie siedziby dostawcy lub jego beneficjenta rzeczywistego.

W związku z powyższym zasadne jest przyjęcie w regulacji jednoznacznego wymogu, zgodnie z którym warunkiem świadczenia usług chmurowych na rzecz administracji publicznej jest nie tylko lokalizacja infrastruktury w ramach EOG, lecz również zapewnienie, że kontrola korporacyjna oraz beneficjent rzeczywisty dostawcy usług pozostają wyłącznie w jurysdykcji państw Europejskiego Obszaru Gospodarczego.

7.1.1. Jak zaprojektować test suwerenności?

Postępująca cyfryzacja państwa sprawia, że infrastruktura cyfrowa staje się warunkiem wykonywania podstawowych funkcji publicznych, od stanowienia i egzekwowania decyzji politycznych, przez wytwarzanie wiedzy instytucjonalnej, po utrzymanie zasobów materialnych państwa. Obowiązujące regulacje krajowe dotyczące infrastruktury krytycznej koncentrują się jednak przede wszystkim na cyberbezpieczeństwie i odporności operacyjnej, pomijając problem zależności technologicznych, ekonomicznych, środowiskowych i jurysdykcyjnych. Proponujemy nowy, warstwowy model suwerenności cyfrowej, który uwzględnia te różne poziomy niezależności państwa. Należy stosować go wobec infrastruktury cyfrowej, oceniając poziom jej krytyczności dla możliwości sprawowania przez państwo podstawowych funkcji. Poniżej opisujemy poszczególne warstwy, następnie przedstawiamy indeks, który pozwala przekształcić je w nowy model kaskadowy zamówień publicznych na infrastrukturę cyfrową. (Model wykorzystuje założenia *Cloud Sovereignty Framework*, ale uzupełnia go o aspekty, które nie zostały w nim ujęte.)

Proponowany przez nas model wychodzi z założenia, że **nie wszystkie elementy infrastruktury cyfrowej mają taki sam poziom znaczenia dla funkcjonowania państwa, a zatem poziom wymaganej kontroli publicznej powinien być stopniowalny i uzależniony od krytyczności danej infrastruktury.** Ocena tej krytyczności wymaga zastosowania sześciu uzupełniających się kryteriów, które odpowiadają warstwom suwerenności.

1. Kryterium operacyjne

Dotyczy znaczenia infrastruktury dla wykonywania zadań publicznych oraz utrzymania ciągłości działania państwa.

Obejmuje zarówno bieżący wpływ systemu na funkcjonowanie instytucji publicznych, jak i jego znaczenie dla zdolności państwa do wyko-

nywania oraz odtwarzania podstawowych funkcji suwerennych w sytuacjach kryzysowych, awaryjnych lub przy długotrwałych zakłóceniach.

Uwzględnia skalę konsekwencji utraty dostępności, możliwość zastąpienia systemu oraz podatność na ataki cybernetyczne i fizyczne.

2. Kryterium jurysdykcyjne

Ryzyko wynikające z podlegania infrastruktury prawu państw trzecich, w szczególności możliwość eksterytorialnego dostępu do danych oraz politycznego wpływu na funkcjonowanie usług cyfrowych.

Kluczowe jest nie tylko zbadanie „gdzie dane są przechowywane", ale jakiemu prawu podlegają firmy, które mają prawnie i technicznie możliwość dostępu do całego stosu usług (dane, klucze, telemetria, personel uprzywilejowany, podwykonawcy i kontrola nad aktualizacjami).

Poziom 1 – jurysdykcja krajowa – Obejmuje infrastrukturę, która pozostaje w pełni poddana prawu krajowemu zarówno w sensie formalnym, jak i operacyjnym, przy czym kluczowe jest nie tylko fizyczne zlokalizowanie danych, lecz także brak istotnych zależności od zagranicznych reżimów prawnych oraz podmiotów mogących podlegać eksterytorialnym obowiązkom ujawniania informacji.

Poziom 2 – jurysdykcja unijna – Obejmuje infrastrukturę podlegającą prawu Unii Europejskiej i państw EOG, przy czym również tutaj istotne jest uwzględnienie potencjalnych punktów styku z reżimami eksterytorialnymi państw trzecich, w szczególności w sytuacji, gdy dostawca usług lub jego podwykonawcy podlegają równolegle jurysdykcji pozaeuropejskiej. Poziom ten oznacza zatem ograniczoną, lecz niepełną autonomię regulacyjną, w której istotne znaczenie ma struktura właścicielska, kontrola technologiczna oraz łańcuch dostaw usług cyfrowych.

Poziom 3 – jurysdykcje państw trzecich – Obejmuje infrastrukturę, która w całości lub w części podlega reżimom prawnym państw spoza UE/EOG, w szczególności w zakresie obowiązków ujawniania danych, dostępu służb publicznych, regulacji bezpieczeństwa narodowego oraz kontroli nad podmiotami świadczącymi usługi cyfrowe. Kluczowe zna-

czenie ma tu nie tylko formalna jurysdykcja siedziby dostawcy, lecz także możliwość eksterytorialnego oddziaływania prawa, w tym dostępu do danych, kluczy kryptograficznych, metadanych, infrastruktury zarządzania usługą oraz personelu uprzywilejowanego.

3. Kryterium ekonomiczne

Obejmuje dwa powiązane, lecz odrębne wymiary oceny infrastruktury cyfrowej. Pierwszym z nich jest **poziom uzależnienia od pojedynczego dostawcy technologicznego oraz występowanie mechanizmów *vendor lock-in***, które ograniczają lub w praktyce uniemożliwiają migrację do alternatywnych rozwiązań. Ocena w tym zakresie powinna uwzględniać nie tylko formalną możliwość przeniesienia systemu, ale również realne koszty migracji, dostępność kompetencji na rynku oraz stopień otwartości architektury technologicznej (w tym dostępność API, formatów danych oraz możliwość samodzielnego utrzymania systemu). Tu również należy ocenić wpływ przyjętego zestawu wytycznych na rozwój krajowego ekosystemu kompetencji i wartości kapitału ludzkiego, czyli potencjału mieszkanek, mieszkańców, przedsiębiorstw i organizacji do wytwarzania znacznej wartości w łańcuchu dostaw i reprodukcji społecznej.

Analiza uzależnienia powinna obejmować również **bezpieczeństwo łańcucha dostaw fizycznych elementów infrastruktury cyfrowej**. Ocena ta powinna uwzględniać stopień koncentracji produkcji, ryzyko zakłóceń geopolitycznych oraz możliwość utrzymania ciągłości funkcjonowania systemów w warunkach kryzysowych. Jednocześnie polityka zamówień publicznych powinna wspierać rozwój krajowych i europejskich kompetencji technologicznych, know-how oraz zdolności produkcyjnych, zwiększających udział lokalnych podmiotów w łańcuchu wartości infrastruktury cyfrowej.

Drugim wymiarem jest **wpływ przyjętego rozwiązania technologicznego na rozwój krajowego ekosystemu kompetencyjnego i produkcyjnego**, rozumianego jako zdolność pracownic, przedsiębiorstw

oraz instytucji do uczestnictwa w tworzeniu wartości w łańcuchu dostaw technologii cyfrowych. W tym ujęciu infrastruktura cyfrowa nie jest wyłącznie kosztem operacyjnym administracji, lecz również narzędziem kształtowania długoterminowych zdolności intelektualnych i gospodarczych państwa czy reprodukcji społecznej.

Oznacza to, że przy wyborze rozwiązań technologicznych w sektorze publicznym należy oceniać nie tylko ich cenę i funkcjonalność, lecz także to, czy dany model wdrożenia umożliwia **rozwój lokalnych kompetencji inżynierskich i administracyjnych**, pozwala na **tworzenie usług i produktów pochodnych przez krajowe podmioty**, wspiera **transfer wiedzy i technologii do krajowego ekosystemu**, czy też przeciwnie – prowadzi do trwałej koncentracji wartości w rękach zewnętrznych dostawców. W tym sensie **infrastruktura cyfrowa staje się również instrumentem polityki rozwojowej**, a nie wyłącznie obszarem zamówień publicznych rozumianych jako zakup usług IT.

Kryterium ekonomiczne obejmuje zarówno właściwości architektoniczne infrastruktury cyfrowej determinujące poziom zależności systemowej, jak i wynikające z nich efekty strukturalne w zakresie organizacji rynku, kompetencji technologicznych oraz dystrybucji wartości w łańcuchu dostaw. Ocena ta powinna obejmować zatem: **interoperacyjność, otwarte standardy, otwarte API, FOSS i *copyleft*** jako mechanizmy kontroli warstwy kodu, umożliwiające zarówno **audytowalność** systemów, jak i **rozwój lokalnych kompetencji, usług oraz produktów o wysokiej wartości dodanej**, a także **zwiększenie efektywności i racjonalności inwestycji publicznych** poprzez unikanie powielania tych samych rozwiązań przy jednoczesnym wspieraniu innowacji budowanych na istniejących komponentach. Kryterium obejmuje również **przenośność danych i systemów, lokalizację łańcucha wartości,** zdolność do odwracalnego wyjścia z systemu bez utraty funkcjonalności (***exit capability***), **kontrolę nad warstwą tożsamości i dostępu oraz stopień koncentracji rynku** dostawców.

4. Kryterium poznawcze (epistemiczne)

Coraz większą rolę odgrywać powinno **kryterium poznawcze (epistemiczne).** Współczesna infrastruktura cyfrowa nie służy już wyłącznie do przechowywania danych, lecz wpływa na procesy komunikacji, obieg informacji, sposób podejmowania decyzji, a w konsekwencji zdolność państwa do autonomicznego przetwarzania wiedzy. Szczególnie widoczne jest to w przypadku usług chmurowych, systemów analitycznych i LLM. Systemy te wpływają nie tylko na techniczne funkcjonowanie administracji, ale również na sposób produkcji wiedzy, organizowania procesów decyzyjnych – im bardziej państwo je wykorzystuje, tym bardziej kluczowe staje się zapewnienie kontroli nad tym, gdzie i według jakich zasad informacje są wytwarzane, przechowywane i przetwarzane. Na przykład narzędzia AI są coraz częściej wykorzystywane do analizy dokumentów, wyszukiwania informacji, tworzenia rekomendacji, automatyzacji pracy urzędniczej czy wspomagania procesów legislacyjnych – z coraz mniejszym udziałem pracowników państwa, a więc z coraz mniejszą możliwością odtworzenia informacji czy logiki podejmowanych decyzji.

Oznacza to, że **kontrola nad tego rodzaju infrastrukturą staje się elementem autonomii państwa porównywalnym z kontrolą nad infrastrukturą energetyczną lub telekomunikacyjną**. W przypadku systemów o wysokim znaczeniu poznawczym państwo powinno móc stawiać **dodatkowe wymagania dotyczące: przejrzystości działania modeli i algorytmów, możliwości audytu sposobu przetwarzania danych, kontroli nad danymi treningowymi oraz systemami treningowymi, lokalizacji** przetwarzania danych, możliwości **wdrażania modeli lokalnie lub w infrastrukturze publicznej, interoperacyjności** i możliwości **migracji** do alternatywnych rozwiązań (otwartych standardów i przenośności), ograniczenia **uzależnienia od pojedynczego dostawcy** technologicznego, czy **stopnia zależności od zewnętrznych systemów poznawczych** oraz ryzyka ich utrwalenia w postaci **epistemicznego** vendor lock-in, a także **zdolności do odtwarzania i weryfikacji procesów decyzyjnych** w czasie, niezależnie od dostawcy technologii.

5. Kryterium środowiskowe

Konieczne jest wprowadzenie (i rozszerzenie w stosunku do propozycji KE) odrębnego **kryterium środowiskowego, czyli oceny infrastruktury cyfrowej pod kątem jej bezpieczeństwa w kontekście zasobów. Znaczenie kluczowe** ma ocena dostępności oraz efektywności wykorzystania wody, energii i innych zasobów w całym cyklu życia systemu oraz, na ile to możliwe, w całym łańcuchu dostaw. Kryterium to powinno być stosowane jako element oceny strategicznej lokalizacji i skali infrastruktury cyfrowej państwa. Zwiększające się wykorzystanie LLM jest **bezpośrednim czynnikiem infrastrukturotwórczym, dlatego analizy powinny objąć** zarówno już istniejące centra danych (i powiązaną infrastrukturę), jak i nowe inwestycje powstające jako efekt tzw. bańki AI (*AI-driven data centers*). Z uwagi na stosunkową nowość tego typu perspektywy aspekt środowiskowy w kontekście centrów danych zostanie omówione szerzej.

Współczesne **centra danych oraz infrastruktura obliczeniowa, w tym LLM, charakteryzują się rosnącym i systemowo niedoszacowanym zużyciem zasobów wodnych**. Najnowsze prognozy wskazują, że w ciągu najbliższych dwóch dekad w skali globalnej centra danych mogą wymagać nawet 150 miliardów metrów sześciennych wody rocznie, co oznacza **24-krotny wzrost względem obecnego poziomu**. Jednocześnie znacząca część wykorzystanej wody nie wraca do lokalnych systemów hydrologicznych, lecz ulega bezpowrotnemu zużyciu, co oznacza realne obciążenie lokalnych zasobów wodnych – mowa tu również o proporcjonalnym, wielokrotnym wzroście zużycia wody. Problem ten ma szczególne znaczenie w kontekście powiązania systemów energetycznych i wodnych. Woda jest niezbędna nie tylko do chłodzenia infrastruktury, ale i do produkcji energii elektrycznej, w szczególności w elektrowniach konwencjonalnych, które nadal stanowią istotną część miksu energetycznego.

Wiele istniejących oraz planowanych instalacji energetycznych lokalizowanych jest na obszarach już dziś doświadczających stresu wodne-

go, co oznacza, że zasoby wodne nie są tam wykorzystywane w sposób zrównoważony. W rezultacie infrastruktura cyfrowa staje się jednym z czynników wzmacniających presję na systemy wodno-energetyczne. Szczególnie istotny jest fakt, że lokalizacja centrów danych oraz pozostałej infrastruktury systemów opartych o LLM często koncentruje się w wybranych regionach metropolitalnych, które jednocześnie należą do obszarów o ograniczonych zasobach wodnych. W przypadku Polski wskazuje się na wysoką koncentrację tego typu infrastruktury w rejonie Warszawy i Mazowsza, które jednocześnie należą do regionów narażonych na pogłębiające się niedobory wody.

Brak systemowych danych dotyczących rzeczywistego zużycia wody i energii przez centra danych w Polsce stanowi istotną lukę w planowaniu strategicznym, ograniczając możliwość oceny długoterminowych skutków rozwoju infrastruktury cyfrowej. W tym kontekście rozwój infrastruktury cyfrowej, w szczególności centrów danych i systemów AI, nie powinien być analizowany wyłącznie w kategoriach bezpieczeństwa cyfrowego i innowacyjności technologicznej, lecz również jako element infrastruktury obciążającej systemy środowiskowe i bezpieczeństwa zasobów naturalnych państwa. **Brak integracji polityki cyfrowej z polityką wodną i energetyczną prowadzi do powstawania ukrytych ryzyk systemowych, które mogą w dłuższej perspektywie przekształcić się w kryzys infrastrukturalny o charakterze gospodarczym, ale także wpływającym na bezpieczeństwo państwa.**

Obecne ramy prawne w Polsce pozostają niewystarczające do uwzględnienia i mitygacji tego ryzyka. W krajowym ustawodawstwie nadal brakuje jasnych definicji kluczowych pojęć, takich jak „ryzyko wodne", „ponowne wykorzystanie wody" (ang. *water reuse*) czy „efektywność wodna". Z tego względu konieczne jest wprowadzenie obowiązku oceny wpływu inwestycji cyfrowych na zasoby wodne i energetyczne w skali lokalnej i krajowej. Ocena ta powinna uwzględniać nie tylko bezpośrednie zużycie zasobów, ale również wpływ łańcucha dostaw, w tym produkcji sprzętu. W tym zakresie możliwe jest wykorzystanie istniejących metodologii, takich jak *Volumetric Water Benefit*

Accounting (Rozliczeniowa ewidencja korzyści wodnych, VWBA 2.0) (Volumetric Water Benefit Accounting, 2019) oraz standard *Alliance for Water Stewardship* (Sojusz na rzecz Zarządzania Zasobami Wodnymi, AWS 3.0) (Alliance for Water Stewardship, 2026), które umożliwiają bardziej precyzyjną ocenę wpływu inwestycji na zasoby wodne w skali całego dorzecza. Ich zastosowanie w ramach zamówień publicznych pozwalałoby na uwzględnienie nie tylko lokalnego poboru wody, lecz również jego systemowych konsekwencji środowiskowych.

Równolegle konieczne jest uwzględnienie aspektu energetycznego, w tym źródeł zasilania centrów danych oraz ich wpływu na stabilność systemu energetycznego. W szczególności należy oceniać stopień samowystarczalności energetycznej infrastruktury cyfrowej oraz jej odporność na zakłócenia, przy jednoczesnym uwzględnieniu wpływu wybranego miksu energetycznego na zużycie wody i obciążenie lokalnych ekosystemów. W praktyce oznacza to konieczność integracji polityki suwerenności cyfrowej z polityką klimatyczną, wodną i energetyczną – **infrastruktura cyfrowa powinna stać się elementem systemu gospodarowania zasobami naturalnymi państwa i podlegać analogicznym zasadom planowania strategicznego jak infrastruktura energetyczna czy wodna**. Podobne wymogi powinny dotyczyć analizy odpowiednich źródeł oraz magazynów energii, które zapewniać mają moce niezbędne do prawidłowego funkcjonowania centrów danych oraz ich stabilność w przypadku awarii lub celowych ataków. Tu uwzględnić należy poziom samowystarczalności energetycznej tych centrów (niezależności od centralnej infrastruktury), który na obecnym etapie zapewniają przede wszystkim OZE w połączeniu z magazynami energii.

Zwrócić należy uwagę, że wybór źródła energii elektrycznej zależnego od chłodzenia wodą oraz wpływ termiczny takiego źródła na środowisko również istotnie wpływa na poziom obciążenia ekosystemu wodnego.

Dodatkowo zasadne jest uwzględnienie wpływu infrastruktury centrów danych na ceny energii elektrycznej oraz stabilność lokalnych systemów energetycznych, co można obserwować na przykładach państw o wysokiej koncentracji tego typu infrastruktury, takich jak Irlandia,

gdzie szybki rozwój centrów danych istotnie wpływa na presję na system energetyczny.

W analizie wpływu infrastruktury cyfrowej na zasoby środowiskowe należy również uwzględnić aspekt długoterminowej elastyczności technologicznej oraz ryzyka nadmiernej specjalizacji infrastruktury. Obecna fala inwestycji w tzw. *AI-driven data centers* opiera się na założeniu stałego i rosnącego zapotrzebowania na moc obliczeniową dla systemów opartych o duże modele językowe, co prowadzi do budowy wysoko wyspecjalizowanej infrastruktury zoptymalizowanej pod określony typ obciążeń obliczeniowych. Infrastruktura ta różni się istotnie od wcześniejszych generacji centrów danych, które były projektowane jako bardziej uniwersalne i elastyczne. W przypadku obecnej generacji obserwuje się wysoką koncentrację zasobów w wyspecjalizowanych układach GPU oraz infrastrukturze chłodzenia dostosowanej do dużej gęstości mocy (ilości energii na jednostkę przestrzeni), co ogranicza możliwość ich alternatywnego wykorzystania w przypadku spadku zapotrzebowania na określone typy obciążeń. Z tego względu zasadne jest uwzględnienie w polityce infrastrukturalnej scenariuszy średnio- i długoterminowych, w których część obecnie budowanej infrastruktury może utracić swoją pierwotną funkcję lub wymagać kosztownej konwersji. Dlatego **kryterium środowiskowe powinno obejmować nie tylko bieżące zużycie zasobów wodnych i energetycznych, lecz również ocenę trwałości funkcjonalnej inwestycji oraz jej zdolności do adaptacji w warunkach zmiany paradygmatu technologicznego, np. poprzez uwzględnienie ryzyka „*stranded infrastructure*[10]”**,

10 Pojęcie *stranded infrastructure* wywodzimy z koncepcji *stranded assets* rozwijanej w ekonomii ekologicznej i w analizach ryzyka inwestycyjnego. Odnosi się do infrastruktury, która przed końcem zakładanego okresu eksploatacji traci znaczną część swojej użyteczności, wartości ekonomicznej lub znaczenia strategicznego wskutek zmian technologicznych, regulacyjnych, rynkowych lub środowiskowych. Przykładem są nowe elektronie węglowe, planowane na kilkadziesiąt lat eksploatacji, które znacznie szybciej stają się nieopłacalne przez nowe regulacje klimatyczne lub tańsze alternatywne źródła energii. Por. Park, H. (2024). Stranded assets. W: D. J. Fiorino, T. A. Eisenstadt, i M. K. Ahluwalia (Red.), *Elgar Encyclopedia of Climate Policy* (s. 198-202).

czyli infrastruktury, która mimo wysokich kosztów budowy i eksploatacji traci swoją użyteczność w wyniku zmian technologicznych lub regulacyjnych.

Kryterium środowiskowe powinno obejmować również wpływ fizycznych komponentów infrastruktury w całym ich cyklu życia. Analizie powinny podlegać w szczególności **koszty środowiskowe i społeczne związane z wydobyciem surowców niezbędnych do produkcji sprzętu teleinformatycznego, układów scalonych, urządzeń sieciowych i systemów magazynowania energii**, w tym ryzyka związane z eksploatacją tzw. minerałów konfliktu oraz koncentracją wydobycia kluczowych surowców w niewielkiej liczbie państw. Równocześnie ocena infrastruktury cyfrowej powinna uwzględniać **stopień zgodności z zasadami gospodarki obiegu zamkniętego**, obejmującymi trwałość urządzeń, możliwość ich naprawy, modernizacji i ponownego wykorzystania, dostępność części zamiennych, a także poziom odzysku surowców po zakończeniu eksploatacji. Z perspektywy suwerenności cyfrowej szczególne znaczenie ma ograniczanie modelu opartego na szybkiej wymianie sprzętu **na rzecz rozwiązań maksymalizujących okres użytkowania infrastruktury oraz zmniejszających zależność od stale rosnącego zużycia zasobów naturalnych i globalnych łańcuchów dostaw**.

Włączenie tego wymiaru do oceny inwestycji publicznych pozwala lepiej **powiązać politykę cyfrową z długoterminową polityką rozwojową państwa**, w której kluczowe znaczenie ma nie tylko bieżąca wydajność systemów, ale również ich elastyczność, rekonfigurowalność oraz odporność na zmianę paradygmatów technologicznych.

6. Kryterium demokratyczne

Ostatnim elementem jest **kryterium demokratyczne**, odnoszące się do wpływu infrastruktury na możliwość realizacji praw człowieka, ale także **realną zdolność obywatelek i obywateli do rozumienia, kontrolowania i współkształtowania infrastruktury cyfrowej**. W tym ujęciu

infrastruktura cyfrowa nie jest tylko narzędziem administracji, lecz systemem tworzącym relacje władzy pomiędzy państwem a obywatelami, kształtującym poziom rozwoju intelektu powszechnego.

Kryterium to obejmuje ocenę wpływu infrastruktury na możliwość realizacji praw człowieka, takich jak dostęp do informacji publicznej, usług publicznych, w tym ochrony zdrowia, pomocy społecznej czy komunikacji, ale również poziom suwerenności jednostek zarówno wobec państwa, jak i podmiotów prywatnych kontrolujących kluczowe warstwy infrastruktury cyfrowej. Istotne jest zbadanie, czy projektowane systemy zwiększają czy ograniczają realną sprawczość użytkowniczek i użytkowników. Sprawczość ta obejmuje następujące warstwy: zdolność do ich rozumienia, audytowania, samodzielnego wytwarzania, modyfikowania oraz zmiany dostawcy bez utraty dostępu do kluczowych usług.

Oznacza to przesunięcie perspektywy z modelu „użytkownika usług cyfrowych" na model „uczestnika i współwłaścicielki infrastruktury cyfrowej", w którym dostęp do wiedzy technologicznej oraz możliwość jej praktycznego wykorzystania stają się elementem infrastruktury demokratycznej. Istotne jest jednocześnie uwzględnienie dbałości o przeciwdziałanie wykluczeniu społecznemu wynikającemu z upowszechnienia technologii cyfrowych i wycofywania się państwa z alternatywnych, „analogowych", rozwiązań.

Z tego względu **kluczowym komponentem polityki suwerenności cyfrowej państwa powinna być systemowa edukacja cyfrowa (edukacja do wolności cyfrowej) obejmująca zarówno dzieci, jak i dorosłych**. Edukacja ta nie powinna ograniczać się do kompetencji użytkowych (obsługi pakietu biurowego), lecz obejmować również rozumienie podstawowych warstw infrastruktury cyfrowej, w tym oprogramowania FOSS, zasad działania systemów opartych o duże modele językowe, a także ich wpływu na środowisko, gospodarkę, procesy decyzyjne i in. Powszechne kompetencje cyfrowe są dziś warunkiem realnej kontroli demokratycznej nad infrastrukturą państwa. Wyłącznie społeczeństwo posiadające zdolność rozumienia podstawowych mechanizmów działania systemów cyfrowych może efektywnie weryfi-

kować, czy polityka suwerenności cyfrowej jest faktycznie realizowana czy jedynie deklarowana.

Kryterium musi też dostrzegać mechanizmy bezpośredniego wpływania na kierunek rozwoju technologii oraz podejmowania decyzji o alokacji wartości wytwarzanej przez usługi cyfrowe. Przykładem takiego rozwiązania jest **stosowanie formy prawnej spółdzielni jako demokratycznego modelu świadczenia usług, współwłasności i współdecydowania**. Spółdzielnie cyfrowe, umożliwiając zrzeszanie zarówno osób fizycznych (np. użytkowników), jak i osób prawnych (np. samorządów czy firm), gwarantują jednocześnie równy głos członkom, co stanowi bezpośrednią realizację demokracji ekonomicznej. **Kryterium demokratyczne powinno rozpoznawać i preferować bardziej pożądane społecznie formy działalności.**

7. Podsumowanie – kryteria klasyfikacji

Proponowany model klasyfikacji infrastruktury cyfrowej państwa opiera się na sześciu uzupełniających się kryteriach oceny krytyczności. Wyodrębnione tu zostały kryteria:

- operacyjne
- jurysdykcyjne
- ekonomiczne
- epistemiczne
- środowiskowe
- demokratyczne

Pierwszym z nich jest kryterium operacyjne, odnoszące się do stopnia, w jakim awaria, utrata integralności lub utrata kontroli nad danym systemem wpływa na zdolność państwa do wykonywania podstawowych funkcji publicznych.

Drugim jest kryterium jurysdykcyjne, obejmujące ryzyko wynikające z podlegania infrastruktury prawu państw trzecich, w szczególności

możliwości ekstraterytorialnego dostępu do danych, wpływu politycznego na funkcjonowanie usług cyfrowych oraz ograniczenia autonomii decyzyjnej państwa.

Trzecim jest kryterium ekonomiczne, dotyczące zarówno poziomu uzależnienia od pojedynczego dostawcy technologicznego (*vendor lock-in*), jak i wpływu infrastruktury na rozwój krajowego ekosystemu kompetencyjnego, przemysłowego i technologicznego (a przez to model rozwoju).

Czwartym jest kryterium poznawcze (epistemiczne), odnoszące się do wpływu infrastruktury cyfrowej na procesy produkcji wiedzy, obieg informacji, organizację procesów decyzyjnych oraz zdolność państwa do autonomicznego przetwarzania danych i wiedzy.

Piątym jest kryterium środowiskowe, obejmujące wpływ infrastruktury cyfrowej na zużycie energii, wody i innych zasobów naturalnych, zarówno w wymiarze lokalnym, jak i globalnym, wraz z oceną długoterminowej trwałości infrastruktury i ryzyka nadmiernej specjalizacji technologicznej.

Ostatnim jest kryterium demokratyczne, odnoszące się do wpływu infrastruktury cyfrowej na możliwość realizacji praw człowieka, poziom sprawczości obywateli oraz zdolność społeczeństwa do rozumienia, kontrolowania i współkształtowania infrastruktury cyfrowej państwa.

Sześć przedstawionych kryteriów tworzy komplementarny model oceny krytyczności infrastruktury cyfrowej, który wykracza poza tradycyjne podejście skupione wyłącznie na cyberbezpieczeństwie i ciągłości operacyjnej. Państwo nie musi sprawować pełnej kontroli nad każdym elementem, jednak im większe znaczenie danej infrastruktury dla autonomii politycznej, zdolności poznawczych instytucji i praw obywateli, tym wyższe powinny być wymagania.

7.1.2. Ocena krytyczności infrastruktury cyfrowej w zamówieniach publicznych

Analiza krytyczności infrastruktury cyfrowej ujawnia, że **decyzje zakupowe w sektorze publicznym** mają konsekwencje wykraczające daleko

poza bieżącą sprawność operacyjną systemów, ponieważ **kształtują one długoterminowe zależności technologiczne, środowiskowe, poznawcze i gospodarcze państw**a. Proponowany przez nas **kaskadowy test suwerenności stanowi odpowiedź na tę lukę – nie jest formalną strukturą prawną ani sztywnym wymogiem, lecz systemem klasyfikacji i wymagań projektowanym w duchu rozwoju *local content* oraz suwerenności cyfrowej**. Jego celem jest **powiązanie decyzji zakupowych z poziomem krytyczności infrastruktury – tak, aby zamówienia publiczne stały się instrumentem świadomego kształtowania krajowego i europejskiego ekosystemu technologicznego, a nie wyłącznie mechanizmem pozyskiwania usług IT przy najniższych kosztach.**

Wyżej opisane kryteria zostały pogrupowane w trzy indeksy, aby uprościć model. Poniżej przedstawiono sugestię rozkładu wag, jednak ich ostateczny układ wymaga osobnego studium.

1. *Criticality Score*

Ocena krytyczności (*Criticality Score*) obejmuje:

- Kryterium operacyjne (wpływ awarii lub zakłócenia systemu na zdolność państwa do działania) Waga –70%
- Kryterium jurysdykcyjne uzupełnia Criticality Score w zakresie, w jakim ryzyka prawne i regulacyjne mogą wpływać na możliwość utrzymania ciągłości działania systemów. Waga – 30%.

2. *Sovereignty Impact Score*

Ocena wpływu na suwerenność (*Sovereignty Impact Score*) obejmuje:

- Kryterium ekonomiczne. Waga – 40%
- Kryterium poznawcze. Waga – 20%
- Kryterium demokratyczne. Waga – 20%

- Kryterium jurysdykcyjne poza wymiarem operacyjnym wpływa również na strukturę zależności polityczno-prawnych państwa wobec innych jurysdykcji. Waga – 20%

3. *Environmental Impact Score*

Ocena wpływu środowiskowego (*Environmental Impact Score*) obejmuje:

- Pobór i zużycie wody i energii (zarówno bezpośredni pobór i zużycie zasobów przez centra danych i infrastrukturę obliczeniową, jak i ich wpływ na lokalne systemy wodno-energetyczne). Waga – 40%
- Warstwa łańcuchów dostaw i surowców obejmuje zdolność systemu do odtwarzania infrastruktury w warunkach zakłóceń dostaw. Uwzględnia ona dostępność surowców krytycznych, możliwość recyklingu komponentów, odporność na koncentrację wydobycia oraz ryzyka geopolityczne związane z łańcuchami dostaw. Waga – 35%
- Stabilność systemu energetycznego i chłodniczego obejmuje zależność infrastruktury cyfrowej od miksu energetycznego, jego odporność oraz konsekwencje lokalizacji centrów danych w kontekście dostępności zasobów. Waga – 25%

7.1.3. Reżimy suwerenności

Poniżej przedstawiamy sposób, w jaki model umożliwia określenie wymaganego poziomu suwerenności w zależności od oceny krytyczności danej infrastruktury. W ramach tego podejścia poszczególnym kategoriom infrastruktury przypisuje się odpowiednie klasy reżimu suwerenności, które różnicują zakres wymagań regulacyjnych i technicznych.

Tabela 3. Reżimy suwerenności

Poziom	Klasa 1 Reżim podstawowy	Klasa 2 Reżim kontrolowany	Klasa 3 Reżim strategiczny	Klasa 4 Rdzeń infrastruktury państwa
Przeznaczenie	Infrastruktura wspierająca funkcjonowanie administracji i usług publicznych	Infrastruktura istotna dla sprawnego wykonywania wybranych funkcji państwa lub dla utrzymania długoterminowej kontroli nad kluczowymi procesami cyfrowymi	Infrastruktura o wysokim poziomie krytyczności operacyjnej oraz istotnym wpływie na zależność technologiczną państwa	Infrastruktura o podstawowym znaczeniu dla ciągłości działania instytucji państwowych oraz kluczowa w zapewnieniu bezpieczeństwa narodowego oraz zarządzania kryzysowego
Wymagany Scoring	CS: 0-50 SIS: 0-50 EIS monitorowany	CS: 50-70 lub SIS: 50-70 EIS: uwzględniany, ale niedecydujący	CS: ≥70 SIS: ≥60 EIS: ≥50	CS: ≥80 SIS: ≥70 EIS: pełna ocena (w tym *stranded infrastructure* i łańcuchy zasobów)
Kluczowe wymogi	Interoperacyjność, API, przenoszalność danych, preferencja rozwiązań FOSS, jurysdykcja w ramach UE	Standard FOSS, interoperacyjność i *exit capability*, obowiązkowa jurysdykcja w ramach UE, audytowanie procesów decyzyjnych i AI, prawo zamawiającego do audytu infrastruktury dostawcy oraz wizji lokalnej na żądanie	Jak w klasie 3, ponadto lokalne wdrażanie modeli AI z pełną kontrolą nad danymi treningowymi, obowiązkowe cykliczne audyty bezpieczeństwa przez uprawniony podmiot krajowy, prawo do wizji lokalnej infrastruktury dostawcy	Jak w klasie 4, ponadto brak *vendor dependency* jako warunek projektowy, lokalizacja danych wyłącznie w jurysdykcji krajowej, obowiązkowe audyty z prawem dostępu do pełnej dokumentacji technicznej i infrastruktury fizycznej, możliwość audytu przez służby państwowe

Źródło: Oprac. własne.

W porównaniu z propozycją z projektu rozporządzenia CADA nasz system uwzględnia więcej warstw infrastruktury cyfrowej, w szczególności ocenę suwerenności pod kątem zależności poznawczej czy środowiskowej, mocniej zaznacza kwestię stosowania FOSS jako narzędzia audytowalności, interoperacyjności i wzmacniania kompetencji technologicznych. Może stać się propozycją nie tyle konkurencyjną wobec CADA, co wspierającą dalsze prace nad rozporządzeniem w kierunku jego pogłębienia i bardziej kompleksowego rozumienia warstw suwerenności. W naszym przekonaniu wprowadzenie powyższego standardu jest konieczne do zabezpieczenia interesu publicznego.

7.2. Certyfikacje zaufanego dostawcy

Jak wskazywano w poprzednich rozdziałach, Krajowy Schemat Certyfikacji nie został dotąd wydany. Art. 7 KSCC wskazuje wprost, że krajowy certyfikat może zostać wydany wyłącznie dla rozwiązań **zapewniających poufność i integralność przetwarzanych danych** na poziomie odpowiednim do potencjalnych cyberzagrożeń. Eksterytorialny dostęp podmiotu z państwa trzeciego do danych, niezależnie od zastosowanych zabezpieczeń technicznych, stanowi znane i realne zagrożenie dla poufności danych. **Ocena jurysdykcyjna i właścicielska** dostawcy powinna być jednym z instrumentów służących weryfikacji ryzyk kryterium już ustanowionego na poziomie ustawy, do którego doprecyzowania w ramach krajowego schematu certyfikacji cyberbezpieczeństwa uprawniony jest minister w drodze rozporządzenia (por. art. 15).

> **Ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa**
> Art. 7. 1. Krajowy certyfikat może zostać wydany dla produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem, które zapewniają dostępność, autentyczność, integralność lub

> poufność przetwarzanych danych lub udostępnianych funkcji lub usług na poziomie odpowiednim do potencjalnych cyberzagrożeń oraz minimalizują znane ryzyka w zakresie cyberzagrożeń.

W przypadku wrażliwych danych i infrastruktury krytycznej kluczowe jest wprowadzenie gradacji wymagań jurysdykcyjnych. **Dla danych o najwyższym stopniu wrażliwości oraz systemów infrastruktury krytycznej państwa dostawca powinien podlegać wyłącznie jurysdykcji polskiej, a infrastruktura i administracja systemem muszą być zlokalizowane na terytorium Polski.** Dla danych o niższym stopniu wrażliwości dopuszczalna jest jurysdykcja unijna, pod warunkiem, że przetwarzanie odbywa się wyłącznie w Europejskim Obszarze Gospodarczym i nie istnieje ryzyko eksterytorialnego dostępu przez podmioty z państw trzecich. Podejście to jest spójne z logiką matrycy klasyfikacji danych zawartej w SCCO i może zostać oparte o tę klasyfikację.

Wymaga to również w przypadku dostawców obsługujących dane wrażliwe oraz infrastrukturę krytyczną także uzyskania wysokiego wyniku testu suwerenności.

Certyfikat zaufanego dostawcy musi gwarantować rzeczywistą kontrolę państwa nad dostarczanymi rozwiązaniami. Ponadto wprowadzenie wymogu posiadania certyfikatu przyspieszy znacznie weryfikację dostawców w procesie zamówień publicznych, unifikując ją do jednostek w tym wyspecjalizowanych i do tego upoważnionych. Instytucje kupujące rozwiązania ICT będą dzięki temu mogły w prosty sposób sprawdzić rzeczywisty poziom zaufania dostawcy.

Jeżeli obecnie obowiązujące przepisy nie umożliwiają jednostkom certyfikującym uwzględniania struktury własnościowej ani jurysdykcji dostawcy w procesie oceny, konieczne jest odpowiednie rozszerzenie ich kompetencji lub wprowadzenie mechanizmu wiążącej współpracy z właściwymi organami państwowymi. Analiza beneficjenta rzeczywistego, struktury właścicielskiej oraz reżimu jurysdykcyjnego stanowi bowiem standardowy element procedur stosowanych przez organy regulacyjne i instytucje sektora finansowego, gdzie tego rodzaju oce-

ny są realizowane rutynowo w ramach obowiązków nadzorczych oraz procedur zgodności.

Przy formułowaniu kryteriów certyfikacyjnych należy jednak koncentrować się na skutkach prawnych i organizacyjnych dla bezpieczeństwa danych, a nie wyłącznie na formalnych cechach podmiotu. **Kryterium jurysdykcyjne powinno być zatem ujmowane przede wszystkim jako ocena odporności na eksterytorialny dostęp do danych, możliwości sprawowania kontroli nad kluczami kryptograficznymi, lokalizacji procesów administracyjnych oraz zdolności do zapewnienia ciągłości i autonomii świadczenia usług.** Struktura właścicielska i podporządkowanie określonym porządkom prawnym pozostają w tym ujęciu istotnymi przesłankami oceny ryzyka, lecz nie stanowią jedynego kryterium certyfikacji.

Jednocześnie krajowy system certyfikacji powinien pozostawać komplementarny wobec europejskich schematów certyfikacyjnych (por. art. 57 aktu o cyberbezpieczeństwie). Do czasu przyjęcia rozwiązań unijnych zapewniających porównywalny poziom ochrony suwerenności cyfrowej certyfikacja krajowa może pełnić funkcję instrumentu przejściowego, odpowiadającego na bieżące potrzeby bezpieczeństwa państwa.

Certyfikat zaufanego dostawcy musi gwarantować rzeczywistą kontrolę państwa nad dostarczanymi rozwiązaniami technologicznymi. Wśród założeń certyfikatu powinny znaleźć się:

- **Suwerenność jurysdykcyjna** (wyrażająca stopień ochrony przed wpływem obcych porządków prawnych, w szczególności poprzez ocenę ryzyka eksterytorialnego dostępu do danych, konfliktów jurysdykcyjnych oraz podporządkowania dostawcy regulacjom państw trzecich).
- **Przejrzystość własnościowa i kontrola nad dostawcą** (polegająca na identyfikacji beneficjenta rzeczywistego, źródeł kontroli kapitałowej oraz podmiotów zdolnych do wywierania istotnego wpływu na działalność dostawcy i świadczone przez niego usługi).

- **Suwerenność infrastruktury i danych** (rozumiana jako zdolność do utrzymania kontroli nad infrastrukturą, procesami administracyjnymi i danymi, obejmująca lokalizację przetwarzania danych, zarządzania systemami oraz kluczowych elementów łańcucha dostaw usług cyfrowych).

7.3. Edukacja do wolności cyfrowej

Zmiana technologiczna nie jest możliwa bez równoległej zmiany w zakresie kompetencji cyfrowych oraz edukacji użytkowniczek i użytkowników, dlatego **państwo musi przeznaczyć środki na systemowe szkolenia pracowników administracji publicznej – zarówno przed wdrożeniem nowych rozwiązań, jak i w trakcie procesu migracji** – co ograniczy opór wobec zmian i ułatwia adaptację do nowego środowiska pracy.

Nie mniej istotne, ze względu na wyzwania opisane w kryterium demokratycznym i poznawczym, jest podniesienie powszechnego poziomu rozumienia, tworzenia, audytowania i modyfikowania infrastruktury cyfrowej. Obejmuje to zarówno **reformę programów nauczania na poziomie szkół podstawowych i średnich,** jak i zmianę kierunków wydatkowania środków publicznych – tak, aby odchodzić od promowania zamkniętych ekosystemów technologicznych na rzecz rozwijania umiejętności krytycznej oceny oraz korzystania z różnorodnych rozwiązań cyfrowych, w tym opartych o FOSS i *copyleft*. Obecnie szkolna edukacja cyfrowa często koncentruje się na użytkowaniu narzędzi dostarczanych przez największych globalnych dostawców technologii, co w praktyce wzmacnia ich dominującą pozycję. Jednocześnie, mimo równoległego akcentowania kwestii takich jak ochrona prywatności, bezpieczeństwo danych czy higiena cyfrowa, uczennice i uczniowie są w dużej mierze w procesie edukacji (podczas zajęć online, poprzez e-dzienniczki czy używanie oprogramowania biurowego w chmurze) osadzani w środowiskach technologicznych, które opierają się na modelach biznesowych zależnych od silnej centralizacji danych i ograni-

czonej przejrzystości ich wykorzystywania. Zamiast uczulać na kwestie suwerenności cyfrowej, szkoła przyzwyczaja dzieci do roli biernych, nadzorowanych odbiorców produktów Big Techów. Reforma powinna zatem przesuwać akcent w stronę nauki programowania, umiejętności oceny i wyboru alternatywnych rozwiązań oraz rozumienia złożoności infrastruktury cyfrowej, w tym jej wpływu na prawa cyfrowe (prawa człowieka w kontekście nowych technologii).

Istotnym mechanizmem wspierającym praktyczny wymiar edukacji cyfrowej może stać się przywrócona ustawowo instytucja spółdzielni uczniowskich. Spółdzielnia uczniowska, prowadzona przez uczennice i uczniów pod opieką nauczycieli, stanowi środowisko, w którym kompetencje cyfrowe nabywane są w działaniu: poprzez prowadzenie działalności, zarządzanie jej zasobami informacyjnymi oraz korzystanie z narzędzi cyfrowych w autentycznym kontekście organizacyjnym. Model ten umożliwia praktyczne kształtowanie umiejętności krytycznego doboru i świadomego wykorzystywania rozwiązań technologicznych, w tym oprogramowania FOSS, łącząc edukację cyfrową z kompetencjami obywatelskimi i przedsiębiorczością.

Taka zmiana stanowiłaby jednocześnie podstawę do wzmocnienia krajowych kadr – zarówno w sektorze publicznym, jak i w gospodarce – zdolnych do projektowania, zamawiania oraz utrzymania infrastruktury cyfrowej w sposób bardziej świadomy, a przez to odporny na uzależnienia zewnętrzne.

7.4. Finansowanie publiczne: BGK i PFR

Rozwój suwerenności cyfrowej wymaga aktywnego wsparcia krajowych przedsiębiorstw technologicznych oraz budowy silnego lokalnego sektora ICT zdolnego do tworzenia konkurencyjnych usług cyfrowych. Szczególne znaczenie mają tutaj instrumenty finansowe państwa, które mogą wspierać m.in. rozwój polskich dostawców oprogramowania i infrastruktury chmurowej[11].

11 Instrumenty wsparcia finansowego należy zaprojektować z wyraźnym zastrzeżeniem zgodności z unijnymi zasadami pomocy publicznej.

Instytucje takie jak Polski Fundusz Rozwoju oraz Bank Gospodarstwa Krajowego są odpowiednimi narzędziami do realizowania tych polityk. Finansowanie kapitałowe ze strony PFR oraz preferencyjne pożyczki i gwarancje BGK mogą umożliwić rozwój krajowych przedsiębiorstw technologicznych, zwiększenie ich zdolności inwestycyjnych oraz skalowanie rozwiązań konkurencyjnych wobec zagranicznych.

Wsparcie powinnzo obejmować szczególnie:

- rozwój usług chmurowych i centrów danych,
- rozwiązania FOSS i interoperacyjne systemy publiczne,
- cyberbezpieczeństwo i technologie infrastrukturalne,
- Partnerstwa Publiczno-Spółdzielcze i spółdzielczość cyfrową,
- projekty strategiczne dla administracji publicznej i infrastruktury krytycznej.

Finansowanie krajowych przedsiębiorstw nie powinno być traktowane wyłącznie jako polityka gospodarcza, ale również jako inwestycja w bezpieczeństwo państwa i odporność cyfrową.

7.5. Podsumowanie narzędzi wdrożeniowych dla państwa

Osiągnięcie suwerenności cyfrowej wymaga długoterminowej i spójnej strategii państwa obejmującej zarówno regulacje rynku cyfrowego, rozwój krajowych kompetencji cyfrowych i finansowe wsparcie kluczowych projektów. Działania, które powinny zostać podjęte przez państwowe instytucje, to:

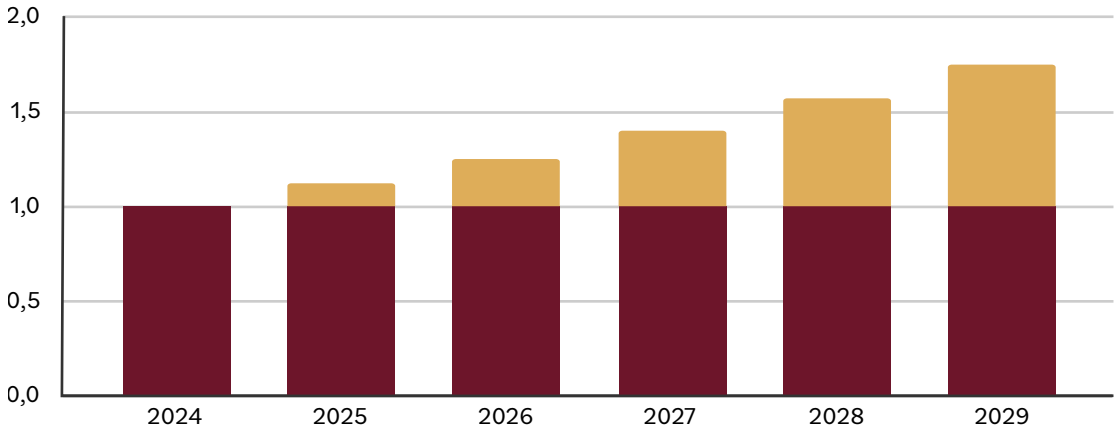
- stosowanie kaskadowego testu suwerenności w zamówieniach publicznych;
- ustanowienie certyfikacji zaufanego dostawcy;
- wprowadzenie edukacji do wolności cyfrowej do podstawy programowej i szkolenia administracji;
- finansowanie publiczne dla krajowych rozwiązań przez BGK i PFR.

Zakończenie

Suwerenność cyfrowa stała się kluczowym warunkiem bezpieczeństwa, odporności gospodarczej i sprawczości państwa. Brak działań w tym obszarze doprowadzi do katastrofalnej w konsekwencjach zależności technologicznej Polski od globalnych dostawców oraz ograniczania konkurencyjności krajowego sektora IT, a w konsekwencji zagrożenia dla bezpieczeństwa państwa.

Koszty ekonomiczne dalszej bezczynności będą rosły. Przyjmując prognozowany wzrost cen usług cyfrowych o 12% rocznie, w ciągu pięciu lat budżet państwa przeznaczony na ten cel wzrośnie o 76%. Nie mając szczegółowych danych na temat tego, czy i jaką część podanego przez ministra Standerskiego kosztu 7 mld zł rocznie (koszt poniesiony w 2024 r. na wytworzenie systemów teleinformatycznych w centralnych podmiotach administracji publicznej, ich utrzymanie i rozbudowę) stanowi zakup usług chmurowych i licencji na oprogramowanie, możemy tylko wskazać na trend. **Dla każdego miliarda wydanego w 2024 r., w 2029 należy prognozować dodatkowe 760 mln zł wydawanych na licencje.**

Wykres. 5. Szacunkowy wzrost kosztów poniesionych przez administrację publiczną na zakup usług chmurowych i licencji na oprogramowanie w perspektywie pięcioletniej dla każdego 1 mld zł (w miliardach złotych)



Źródło: Oprac. własne.

Doświadczenia państw takich jak Francja, Niemcy czy Wielka Brytania pokazują, że możliwe jest prowadzenie aktywnej polityki wspierania interoperacyjności, FOSS oraz lokalnych dostawców technologicznych przy jednoczesnym zachowaniu zgodności z regulacjami Unii Europejskiej i utrzymaniu wysokiego poziomu bezpieczeństwa cyfrowego. Kluczowe znaczenie będzie miało stworzenie ram regulacyjnych, zakupowych oraz programów finansowych, które pozwolą Polsce rozwijać własne kompetencje technologiczne, wzmacniać odporność cyfrową państwa oraz budować konkurencyjny rynek usług cyfrowych.

Cyfrowa suwerenność stanowi konieczność w świecie niestabilności geopolitycznej. Jednocześnie **jest historyczną szansą rozwojową dla państw znajdujących się, jak Polska, na (pół)peryferiach globalnego systemu gospodarczego**. Przejście od pozycji zależności technologicznej do współkształtowania architektury cyfrowej może umożliwić częściowe przesunięcie w kierunku centrum systemu wytwarzania wartości dodanej. Charakter tej transformacji ma jednak ograniczony horyzont czasowy.

Wewnątrz Unii Europejskiej trwa wyścig suwerennościowy, co sprawia, że tempo i jakość decyzji politycznych, które podejmą polskie władze, będą miały kluczowe znaczenie dla wykorzystania tej fazy przejściowej w procesie budowania nowego modelu rozwoju Polski.

Spis wykresów i tabel

Bibliografia

Adach, O. (2024, 31 stycznia). Munich's Long History with Open Source in Public Administration. *Open Source Observatory*. https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/document/munichs-long-history-open-source-public-administration

Ahern, J. (2023, 12 stycznia). Open source software is transforming healthcare. *Opensource*. https://opensource.com/article/23/1/open-source-software-transforming-healthcare

Alliance for Water Stewardship. AWS 3.0. (2026). https://a4ws.org/wp-content/uploads/2026/03/AWS_Standard-3.0_2026-_English.pdf

Asterès. (2026). *From technological dependency to economic capture: The cost of cloud & software services inflation to Europe*. https://www.cigref.fr/from-technological-dependency-to-economic-capture-the-cost-of-cloud-software-services-inflation-to-europe

Asterès. (2025). *Technological dependence on American software and cloud services: an assessment of the economic consequences in Europe*. https://www.cigref.fr/technological-dependence-on-american-software-and-cloud-services-an-assessment-of-the-economic-consequences-in-europe

Brecht, Ch. (2024, 8 października). Gesellschaft für Informatik warnt vor Delos Cloud. *Behörden Spiegel*. https://www.behoerden-spiegel.de/2024/10/08/gesellschaft-fuer-informatik-warnt-vor-delos-cloud/

Clarifying Lawful Overseas Use of Data Act or CLOUD Act. (2018). Public Law 115–141 by the 115th Congress. https://www.govinfo.gov/content/pkg/PLAW-115publ141/pdf/PLAW-115publ141.pdf

Desmarais, A. (2025). Two city governments in Denmark are moving away from Microsoft amid Trump and US Big Tech concerns. *Euronews*. 12.06.2025. https://www.euronews.com/next/2025/06/12/two-city-governments-in-denmark-are-moving-away-from-microsoft-amid-trump-and-us-big-tech-

Carlson, J. (2024, 3 kwietnia). Licensing and pricing updates for on-premises server products coming July 2025. *Microsoft 365 Blog*. https://techcommunity.microsoft.com/blog/microsoft_365blog/licensing-and-pricing-updates-for-on-premises-server-products-coming-july-2025/4400174/replies/44307

Central Digital and Data Office. (2012, 6 listopada). *Digital Efficiency Report*. https://www.gov.uk/government/publications/digital-efficiency-report/digital-efficiency-report

Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, 132 Stat. 1213 (2018). https://www.congress.gov/bill/115th-congress/senate-bill/2383/text

Data Center SecNumCloud: Souveraineté & Sécurité Étatique. (b.d.). *Data Cube Systems*. https://www.datacube-systems.com/conformite/data-center-secnumcloud

Digital Marketplace. https://www.applytosupply.digitalmarketplace.service.gov.uk/

Draouil, M. (2025). The End of Windows': How France's GendBuntu Signals a Shift from Costly, Patch-Plagued Systems. *Medium*. https://medium.com/@majdidraouil/the-end-of-windows-how-france-s-gendbuntu-signals-a-shift-from--costly-patch-plagued-systems-2086aee86fe9

DWS News. (2025, 18 listopada). *Prezydent Emmanuel Macron przemawia na Szczycie Cyfrowym UE poświęconym technologii i innowacjom.* https://www.youtube.com/watch?v=TLRMy6xC3Mo

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (dyrektywa NIS 2). Dz.U.UE.L.333 z 27.12.2022, s. 80–152. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych (dyrektywa CER). Dz.U.UE.L.2022.333.164. https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022L2557

Elée. (2025). *Note stratégique. Tendances du marché logiciels & cloud*. .[Broszura]. https://elee.com/sites/elee-site/files/publication/file/elee-note-strategique--tendances-du-marche-logiciels-cloud_0.pdf

Élysée [Portal Pałacu Elizejskiego]. (2025, 18 listopada). *Summit on European Digital Sovereignty Delivers Landmark Commitments for a more competitive and sovereign Europe*. [Komunikat]. https://www.elysee.fr/en/emmanuel-macron/2025/11/18/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe

Endicott, S. (2020, 04 marca). Microsoft offers premium Teams for free over the next six months due to coronavirus. *Windows Central*. www.windowscentral.com/microsoft-offers-premium-teams-free-over-next-six-months-due-coronavirus

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978). https://www.govinfo.gov/content/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf

France swaps Windows for Linux in sovereignty push. (2026). *Innovation Origins Plus*. https://ioplus.nl/en/posts/france-swaps-windows-for-linux-in-sovereignty-push

Gabriel, P., Jaśkowiec, D., Krzywonos-Strycharska, H., Niedźwiedzki, J., Siemaszko, R., Szopiński, H. i Zawieja, B. (2026, 16 kwietnia). *Interpelacja nr 16665 w sprawie inwestycji i reform podnoszących poziom suwerenności cyfrowej Polski w kontekście rosnącego deficytu w handlu produktami cyfrowymi.* https://sejm.gov.pl/Sejm10.nsf/interpelacja.xsp?typ=INT&nr=16665

G-Cloud Digital Marketplace. (b.d). https://www.applytosupply.digitalmarketplace.service.gov.uk/

Government Digital Service (GDS). (b.d.). https://www.gov.uk/government/organisations/government-digital-serviceGUS. Słownik pojęć. (b.d.). Sektor ICT. W: *GUS. Pojęcia stosowane w statystyce publicznej*. https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1858,pojecie.html

Hof, L. (2026, 13 maja). FR#162 – EU Regulation Won't Save Open Social Networks. *Connected Places*. https://connectedplaces.online/reports/fr162-eu-regulation-wont-save-open-social-networks/

ICC to ditch Microsoft following US sanctions. (2025, 31 października). *Irish Legal News*. https://www.irishlegal.com/articles/icc-to-ditch-microsoft-following-us-sanctions

Joint Call for a Sovereign and Resilient European Cloud Policy. (2026, 17 marca). https://www.cispe.cloud/website_cispe/wp-content/uploads/2026/03/Cloud-CEOs-Joint-Letter-March-17-2026-FINAL.pdf

Kattel, R. i Ville T. (2023). The Case of the UK's Government Digital Service: The Professionalisation of a Paradigmatic Public Digital Agency. *Digital Government: Research and Practice*, 4(4), 1–15. https://doi.org/10.1145/3630024

Komisja Europejska. (2020, 19 lutego). *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów. Europejska strategia w zakresie danych (Data Strategy Gaia-X).* https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52020DC0066

Komisja Europejska. (2025). *Cloud Sovereignty Framework: Sovereignty effectiveness assurance levels (SEAL)* (Version 1.2.1). Urząd Publikacji Unii Europejskiej. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

Komisja Europejska. (2026, 17 kwietnia). *Commission advances cloud sovereignty through strategic procurement*. https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en

Kopeć J. (2025). *Zamówienia na pozór otwarte. Nierówne szanse producentów oprogramowania w zamówieniach publicznych polskiej administracji*. Instrat Policy Note 02/2025. https://instrat.pl/wp-content/uploads/2025/12/Instrat-Policy-Note-03-2025-Zamowienia-na-pozor-otwarte_.pdf

Kuo, L. i Davidson, H. (2020, 11 czerwca). Zoom shuts accounts of activists holding Tiananmen Square and Hong Kong events. *The Guardian*. https://www.theguardian.com/technology/2020/jun/11/zoom-shuts-account-of-us-based-rights-group-after-tiananmen-anniversary-meeting

Leistner, A. (2026, 24 kwietnia). France moves public health data from Microsoft to French cloud provider. *Euronews*. https://www.euronews.com/health/2026/04/24/france-moves-public-health-data-from-microsoft-to-french-cloud-provider

Levin, S. i Sweney, M. (2026, 23 stycznia). TikTok announces it has finalized deal to establish US entity, sidestepping ban. *The Guardian*. CET https://www.theguardian.com/us-news/2026/jan/22/tiktok-us-venture-oracle

„Local Content. Z korzyścią dla Polski". Wspieramy krajowe firmy. Budujemy gospodarkę. (2026). https://www.gov.pl/web/aktywa-panstwowe/local-content-z-korzyscia-dla-polski-wspieramy-krajowe-firmy-budujemy-gospodarke

Matuszewski, M. (2026, 08 kwietnia). *Interpelacja nr 16344 w sprawie efektywności wydatków na cyfryzację administracji. Zgłaszający Marek Matuszewski.* https://www.sejm.gov.pl/sejm10.nsf/interpelacja.xsp?typ=INT&nr=16344

Meijer, R. (2025, 27 marca) Open Letter to Meta: Support True Messaging Interoperability with XMPP. *XMPP*. https://xmpp.org/announcements/open-letter-meta-dma/

Microsoft. (2026, 16 lutego). *Microsoft 365 Pricing and Packaging Updates* [Komunikat]. https://www.microsoft.com/en-us/licensing/news/2026-m365-packaging-pricing-updat

Ministerstwo Cyfryzacji. (b.d.). Projekt aktualizacji Standardów Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO). Serwis Rzeczypospolitej Polskiej. https://www.gov.pl/web/cyfryzacja/standardy-cyberbezpieczenstwa-chmur-obliczeniowych

Ministerstwo Cyfryzacji. Portal Interoperacyjności i Architektury. (b.d.). *System Inwentaryzacji Systemów Teleinformatycznych*. Serwis Rzeczypospolitej Polskiej. https://www.gov.pl/web/ia/system-inwentaryzacji-systemow-teleinformatycznych-sist

Nagle, F. (2019). *Government Technology Policy, Social Value, and National Competitiveness*. SSRN. Harvard Business School Strategy Unit Working Paper No. 19-103. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3355486

Narodowe Standardy Cyberbezpieczeństwa. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), v. 1.00 – luty 2020. (2020). https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://crypto.stanford.edu/portia/papers/privacy_in_context.pdf

OChK Cloud. (b.d.). https://ochk.cloud/pl/produkty/google-cloud

Oleszczuk-Zygmuntowski, J. (2025). *Cyfrowy bilans Polski. Jak zmienić uzależnienie w suwerenność?* Centrum Łukasiewicz Sieć Badawcza, Warszawa. https://lukasiewicz.gov.pl/wp-content/uploads/2025/12/Cyfrowy_bilans_Polski.pdf

Park, H. (2024). Stranded assets. W: D. J. Fiorino, T. A. Eisenstadt, i M. K. Ahluwalia (Red.), *Elgar Encyclopedia of Climate Policy* (s. 198–202). Edward Elgar. https://doi.org/10.4337/9781802209204.ch37

Paul. (2024, 01 października). Microsoft Announces SPLA Price Increases for 2025: What You Need to Know. *Altaris Claud*. https://altariscloud.com/microsoft-announces-spla-price-increases-for-2025-what-you-need-to-know/

Philpot, J. (2024, 05 września). Changes to the EU Cloud Services Cybersecurity Certification Scheme put EU citizens' data at risk: A Call for Digital Sovereignty. *European Digital SME Alliance*. https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty/

Piquard, A. (2025, 01 maja). Le „cloud souverain" français et européen, un défi face à la puissance américaine. *Le Monde*. https://www.lemonde.fr/economie/article/2025/05/01/le-cloud-souverain-francais-et-europeen-un-defi-face-a-la-puissance-americaine_6602116_3234.html

Polska Chmura. (2026, 13 lutego). *Polska Chmura apeluje do Prezydenta w obronie cyfrowej suwerenności Polski*. [Komunikat]. https://polska-chmura.pl/polska-chmura-apeluje-do-prezydenta-w-obronie-cyfrowej-suwerennosci-polski/

Prace koncepcyjne nad projektem ustawy o chmurze obliczeniowej w administracji. (2025, 17 kwietnia). *Warto Wiedzieć*. https://wartowiedziec.pl/attachments/article/76327/2025.04%20Prezentacja%20na%20ZSI%20-%20ustawa%20chmurowa%20%20prace%20koncepcyjne.pdf

Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act: CADA). (2026). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52026PC050

Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, 138 Stat. 895 (2024). https://www.govinfo.gov/content/pkg/PLAW-118publ50/pdf/PLAW-118publ50.pdf

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). Dz.U. L 151 z 7.6.2019, s. 15–69 z późn. zm. https://eur-lex.europa.eu/eli/reg/2019/881/oj/pol

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych DSE). Dz.U. L 277 z 27.10.2022, s. 1–102. https://eur-lex.europa.eu/eli/reg/2022/2065/oj/pol

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/1925 z dnia 14 września 2022 r. w sprawie kontestowalnych i uczciwych rynków w sektorze cyfrowym (akt o rynkach cyfrowych DMA). Dz.U. L 265 z 12.10.2022, s. 1–66. https://eur-lex.europa.eu/eli/reg/2022/1925/oj/pol

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1781 z dnia 13 września 2023 r. w sprawie ustanowienia ram dotyczących środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników (akt w sprawie czipów). Dz.U. L 229 z 18.9.2023, s. 1–53. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32023R1781

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt w sprawie sztucznej inteligencji, AI Act). Dz.U. L, 2024/1689, 12.7.2024. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32024R1689

Rozstrzygnięcie Międzynarodowego Trybunału Arbitrażowego w sprawie Juvel LTD i Bithell Holdings LTD. (2019, 01 marca). https://www.gov.pl/web/cyfryzacja/rozstrzygniecie-miedzynarodowego-trybunalu-arbitrazowego-w-sprawie-juvel-ltd-i-bithell-holdings-ltd

Service Provider License Agreement (SPLA). (b.d.). https://download.microsoft.com/documents/pl-pl/files/SPLA_ref_card_PL_final.pdf

Sneddon, J. (2025, 17 czerwca). Denmark's Government Ditches Microsoft for Open Source. *OMG Ubuntu*. https://www.omgubuntu.co.uk/2025/06/denmark-government-replaces-microsoft-with-linux-libreoffice

„Sovereignty washing": quand le cloud se pare d'un label européen trompeur. (b.d.). L'Echo. https://www.lecho.be/opinions/general/expert-sovereignty-washing-quand-le-cloud-se-pare-d-un-label-europeen-trompeur/10646005.html

Spataro, J. (2021, 19 sierpnia). New pricing for Microsoft 365. *Microsoft*. https://www.microsoft.com/en-us/microsoft-365/blog/2021/08/19/new-pricing-for--microsoft-365/

Standerski D. (2026, 24 maja). *Odpowiedź Sekretarza Stanu Dariusza Standerskiego dot. pisma z 22 kwietnia br. Posłów na Sejm RP Panów Rafała Siemaszko, Bartosza Zawiei, Patryka Gabriela, Jacka Niedźwiedzkiego, Pani Henryki Krzywonos-Strycharskiej, Panów Dominika Jaśkowiec oraz Henryka Szopińskiego w sprawie inwestycji i reform podnoszących poziom suwerenności cyfrowej Polski w kontekście rosnącego deficytu w handlu produktami cyfrowymi (interpelacja nr 16665)*. https://sejm.gov.pl/INT10.nsf/klucz/ATTDUFJAN/%24FILE/i16665-o2.pdf

Standerski, D. (2026, 25 maja). *Odpowiedź Sekretarza Stanu Dariusza Standerskiego dot. pisma z 8 kwietnia br. Posła na Sejm RP Pana Marka Matuszewskiego w sprawie efektywności wydatków na cyfryzację administracji (interpelacja nr 16344)*. BM.WP.057.70.2026. https://sejm.gov.pl/INT10.nsf/klucz/ATTDUGHKR/%24FILE/i16344-o1.pdf

Stephens, J. (2024, 13 czerwca). Unlocking Value: Principles of Total Cost Ownership. *Gartner*. https://www.gartner.com/en/documents/5505795

System Operacyjny GNU. (2026). *Co to wolne oprogramowanie?* https://www.gnu.org/philosophy/free-sw.html

Takagi, P. (2025, 03 listopada). Huawei grozi arbitrażem. Czy Polska stanie przed międzynarodowym trybunałem?. *Forbes Polska*. https://www.forbes.pl/opinie/huawei-grozi-arbitrazem-czy-polska-stanie-przed-miedzynarodowym-trybunalem/fn94lvr

Tech Giants and Giant Slayers: The case for Digital Sovereignty and the Digital. (2026, 14 kwietnia). https://www.openrightsgroup.org/publications/tech-giants-and-giant-slayers-the-case-for-digital-sovereignty-and-the-digital-commons/

Tewari, S. i Jamali, L. (2026, 23 stycznia). *TikTok closes deal to split US app from global business*. https://www.bbc.com/news/articles/c3edd1l328lo

Thoma, J. (2017, 20 lutego). Limux. Die tragische Geschichte eines Leuchtturm-Projekts. *Golem*. https://www.golem.de/news/limux-die-tragische-geschichte-eines-leuchtturm-projekts-1702-126230.html

Traktat o funkcjonowaniu Unii Europejskiej. (2016). https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0018.01/DOC_3&format=PDF

Traktat o Unii Europejskiej. (2016). Dz.U. C 202 z 7.6.2016, s. 1–388. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:12016ME/TXT

Ubuntu. (2010, 10 listopada). *La Gendarmerie Nationale upgrades 85,000 PCs to Ubuntu Desktop Edition* [Komunikat]. Canonical Ubuntu. https://ubuntu.com/blog/la-gendarmerie-nationale-upgrades-85000-pcs-to-ubuntu-desktop-edition

Udhayakumar, G. K. (2026, 04 kwietnia). VMware pricing after Broadcom: The 800–1,500% price shock, what changed and your real alternatives in 2025. *Software Guide*. https://softwarepricingguide.com/vmware-pricing-after--broadcom-the-800-1500-price-shock-what-changed-and-your-real-alternatives-in-2025/

Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa" (WIIP). (2019). Monitor Polski. Dziennik Urzędowy Rzeczpospolitej Polskiej, Warszawa, dnia 24 września 2019 r. Poz. 862. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190000862/O/M20190862.pdf

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. (Dz. U. 2007 Nr 89 poz. 590). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. (Dz. U. 2018 poz. 1560). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf

Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych. (Dz. U. 2019 poz. 2019). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20190002019/U/D20192019Lj.pdf

Ustawa z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa. (Dz.U. 2025 poz. 1017). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20250001017/T/D20251017L.pdf

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. (Dz.U. 2007 nr 89 poz. 590). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/T/D20070590L.pdf

Vaughan-Nichols, S. (2025). German state replaces Microsoft Exchange and Outlook with open-source email. *ZDNET*. https://www.zdnet.com/article/german-state-replaces-microsoft-exchange-and-outlook-with-open-source-email/

Visa de sécurité. (b.d.). Agence Nationale de la Sécurité des Systèmes d'Information [ANSSI]. https://cyber.gouv.fr/offre-de-service/solutions-certifiees-et-qualifiees/comprendre-levaluation-de-securite/visa-de-securite/

Warso, Z. i Singh, A. (2026, 19.03). Infrastructure as a foundation for digital sovereignty. Policy Building Blocks for the Digital Commons #1; Open Future policy brief. *Open Future*. https://openfuture.eu/wp-content/uploads/2026/03/260319_Cloud-infrastructure-as-a-foundation-for-digital-sovereignty-.pdf

Wawrzyniak, B., Zygmuntowski, J. i Lamański, F. (2020). Polska suwerenna cyfrowo. Regulacje na rzecz sprawiedliwej i konkurencyjnej gospodarki cyfrowej. *Instrat Policy Paper* 06/2020. https://instrat.pl/wp-content/uploads/2020/10/Polska-suwerenna-cyfrowo-Instrat.pdf

Web3 Foundation. (2026). *The Hidden Price of Free: What Your Data Is Really Worth. The Personal Economics of Big Tech and AI. A Web3 Foundation White Paper*. https://web3.foundation/hidden-price-of-free/web3-foundation-hidden-price-of-free-white-paper.pdf

Weigl, L. i Guzik, A. (2025). In Brussels we trust? Exploring corporate resistance in platform regulation. *Law, Innovation and Technology*, 17(1). S. 335–365. https://doi.org/10.1080/17579961.2025.2470588

Volumetric Water Benefit Accounting. VWBA 2.0. (2019). https://www.wri.org/research/volumetric-water-benefit-accounting-2-0

Biogramy

Michał Myśliwiec to student Metod Ilościowych w Szkole Głównej Handlowej i Stosunków Międzynarodowych na Uniwersytecie Warszawskim. W roku akademickim 2024/2025 pełnił rolę wiceprzewodniczącego w Studenckim Kole Naukowym Ekonomii Politycznej. Członek Polskiej Sieci Ekonomii oraz współautor raportu *Cyfrowy bilans Polski*. Zajmuje się tematyką ekonomii cyfrowej i ekonomii politycznej.

Maria Świetlik jest dyrektorką zarządzającą Polskiej Sieci Ekonomii. Zajmuje się tematyką wolnego internetu i praw cyfrowych, globalnej sprawiedliwości i feminizmu socjalnego. Publicystka, koordynatorka projektów badawczych i redaktorka książek dot. praw cyfrowych (m.in. Eben Moglen *Wolność w chmurze*, J. Oleszczuk-Zygmuntowski *Kapitalizm w sieci*).

Dr Jan Oleszczuk-Zygmuntowski to ekonomista i przedsiębiorca społeczny zainteresowany złożonymi systemami, ekonomią polityczną technologii oraz gospodarką cyfrową. Współprzewodniczący Polskiej Sieci Ekonomii i Prezes Zarządu PLZ Spółdzielni, operatora centrum technologii spółdzielczych CoopTech Hub. Wykładowca Akademii Leona Koźmińskiego na kierunku Zarządzanie i AI w Cyfrowym Społeczeństwie. Założyciel i w latach 2015-2020 prezes zarządu Fundacji Instrat, progresywnego think-tanku. Doświadczenie zdobywał m.in. w Polskim Funduszu Rozwoju. Absolwent Szkoły Głównej Handlowej w Warszawie, stypendysta G20 Global Solutions, British Council, Møller Institute, Open Future Foundation i FEPS. Autor *Kapitalizmu Sieci*, książki nominowanej do nagrody Economicus 2020. Ambasador DigitalEU.

Ekonomia w służbie społeczeństwu

Łączymy badaczki i badaczy
na rzecz rozwoju
społeczno-gospodarczego.
Wspieraj nas i regeneruj
z nami Polskę!

www.plse.org.pl

Polska Sieć
Ekonomii