



Instytut
Poznański

Suwerenność Cyfrowa

Między autonomią
a pragmatyzmem

dr Andrzej Kozłowski

Wydawca



Instytut Poznański to dynamicznie rozwijający się think tank zajmujący się sprawami miejskimi, samorządowymi, społecznymi i międzynarodowymi.

Naszą misją jest wspieranie rozwoju społeczeństwa obywatelskiego i wzmacnianie oddolnej aktywności społecznej obywateli. Chcemy to osiągnąć, dzieląc się wiedzą i doświadczeniem. Pierwszym miejscem naszej działalności jest Poznań, ale perspektywa sięga poza granice miasta, a nawet kraju.

Poznaj nasze projekty!



poznanski.org/#projekty

Instytut Poznański, ul. Młyńska 14, 61-730 Poznań

Numer KRS: 0000752367

NIP: 7831789732

REGON: 381529633

www.poznanski.org | instytut@poznanski.org



ISBN 978-83-962475-4-4



Raport powstał we współpracy z firmą:



Partner Medialny: **CyberDefence 24**

Poznań, luty 2026

Wprowadzenie

Suwerenność technologiczna stała się jednym z kluczowych tematów debaty publicznej w Unii Europejskiej i państwach członkowskich. Dotyczy ona nie tylko technologii jako takiej, lecz także bezpieczeństwa państwa, stabilności gospodarki, ciągłości usług publicznych oraz zaufania obywateli do instytucji.

Cyfryzacja administracji, rosnąca rola chmury obliczeniowej i sztucznej inteligencji, a także dynamiczny wzrost zagrożeń w cyberprzestrzeni powodują, że decyzje technologiczne przestały mieć charakter wyłącznie techniczny. Stały się decyzjami strategicznymi, których skutki są długofalowe i trudne do odwrócenia.

W ostatnich latach w Europie coraz częściej pojawia się narracja suwerenności rozumianej jako technologiczna samowystarczalność lub ograniczanie współpracy z globalnymi dostawcami technologii. Takie podejście, choć intuicyjnie atrakcyjne, w praktyce niesie ze sobą istotne ryzyka: wzrost kosztów, spadek innowacyjności oraz pozorne poczucie bezpieczeństwa.

Jednocześnie rzeczywistość cyfrowa ma charakter transgraniczny. Dane, systemy i zagrożenia nie zatrzymują się na granicach państw. Skala współczesnych wyzwań sprawia, że żadne państwo europejskie nie jest w stanie samodzielnie budować pełnego ekosystemu technologicznego bez współpracy międzynarodowej.

Ten raport powstał w odpowiedzi na potrzebę odejścia od uproszczonych narracji i proponowania podejścia pragmatycznego, opartego na realnych możliwościach państw, analizie ryzyk oraz świadomym zarządzaniu zależnościami technologicznymi.



Jan Zujewicz

Prezes Instytutu Poznańskiego

EXECUTIVE SUMMARY

STRESZCZENIE

Cel raportu

Celem raportu jest zaproponowanie praktycznego modelu suwerenności technologicznej, który wzmacnia bezpieczeństwo i odporność państwa, nie prowadząc jednocześnie do izolacji technologicznej ani utraty konkurencyjności.

Raport odpowiada w szczególności na następujące pytania:

- ▶ czym w praktyce jest suwerenność technologiczna i czym nie jest,
- ▶ jakie obszary państwo powinno kontrolować bezpośrednio,
- ▶ kiedy współpraca z globalnymi dostawcami jest uzasadniona i bezpieczna,
- ▶ jakie ryzyka wiążą się z niekontrolowaną zależnością technologiczną,
- ▶ jak projektować polityki publiczne w sposób realistyczny i skalowalny.

Raport ma charakter analityczno-strategiczny i jest adresowany do decydentów publicznych, regulatorów, ekspertów oraz interesariuszy rynku technologicznego.

Streszczenie

Nowoczesna suwerenność technologiczna nie polega na eliminowaniu zagranicznych technologii ani na budowie pełnej autarkii. Polega na zdolności państwa do podejmowania świadomych decyzji technologicznych, kontroli kluczowych elementów systemów oraz możliwości zmiany dostawców bez utraty ciągłości działania.

Raport wskazuje, że:

- ▶ pełna samowystarczalność technologiczna państw UE jest ekonomicznie i operacyjnie nieosiągalna,
- ▶ kluczowe znaczenie ma kontrola nad danymi, architekturą systemów i mechanizmami bezpieczeństwa,
- ▶ interoperacyjność, standardy i certyfikacja są skuteczniejsze niż zamknięte rozwiązania narodowe,
- ▶ nadmierny vendor lock-in, niezależnie od pochodzenia dostawcy, stanowi ryzyko systemowe,
- ▶ racjonalnie zarządzana współpraca technologiczna wzmacnia odporność państwa i gospodarki.

Raport proponuje model „kontrolowanej współpracy”, który łączy interesy bezpieczeństwa państwa z realiami rynku technologicznego i dynamiką globalnych innowacji.

O autorze

Andrzej Kozłowski, doktor nauk politycznych. Prowadził wykłady i konsultacje na Uniwersytecie Łódzkim, Wyższej Szkole Informatyki Stosowanej i Zarządzania w Warszawie oraz Collegium Civitas z zakresu bezpieczeństwa międzynarodowego, dezinformacji, terroryzmu i cyberbezpieczeństwa. Uczestnik programów: IV LP Departamentu Stanu: 21st Century Changemakers: Information Technology Leaders Explore Cyber Security Strategies, Fullbright Journalistic Challenges and Practices. Kierował zespołem analizy trendów narracyjnych i fact-checkingu w NASKu oraz biurem analiz Fundacji im. Kazimierza Pułaskiego. Pełnił rolę redaktora naczelnego portalu CyberDefence24.pl.



SPIS TREŚCI

Wstęp	6
1. Suwerenność cyfrowa	7
2. Pragmatyczne podejście do koncepcji cyfrowej suwerenności	12
3. Unia Europejska na drodze do realizacji pragmatycznej suwerenności	18
4. Trudna droga budowania suwerenności cyfrowej w obszarze 5G	27
Zakończenie	30

Wstęp

Wyobraźmy sobie sytuację, w której budzimy się jutro i nie mamy dostępu do żadnych aplikacji, danych, informacji czy chmury, a nasze smartfony nie działają – to oczywiście apokaliptyczny scenariusz wycofania się amerykańskich i chińskich firm technologicznych z Europy. Technologicznej hegemonii USA doświadczył na własnej skórze francuski sędzia Nicolas Guillou z Międzynarodowego Trybunału Karnego, który został objęty amerykańskimi sankcjami. Na ich skutek wszystkie konta i profile na serwisach takich jak Amazon, Airbnb, PayPal zostały zamknięte. Nie może on korzystać z systemów płatności American Express, Visa i Mastercard. W konsekwencji jego codzienne funkcjonowanie uległo znacznemu i dotkliwemu utrudnieniu¹. Niestety Unia Europejska nie jest i długo nie będzie przygotowana na takie scenariusze. Co więcej, europejskie rozwiązania technologiczne nie są stosowane nawet w najbardziej wrażliwych sektorach, gdzie dochodzi do obiegu informacji niejawnych, co stwarza uzasadnione zagrożenie. Dlatego też w ramach UE coraz częściej dyskutuje się o konieczności stworzenia cyfrowej suwerenności. Jest to ogromne wyzwanie, wiążące się z koniecznością zastąpienia warstwy hardwarowej, softwarowej, usług oraz licznych inwestycji w innowacje, które pozwolą na tworzenie nowych technologii. Szacuje się, że stworzenie pełnej suwerenności cyfrowej może kosztować nawet 3,6 biliona euro². Niewłaściwe kroki na drodze do suwerenności cyfrowej mogą jednak prowadzić do utrudnionego dostępu lub nawet braku dostępu do ważnych usług. Obserwujemy to na przykładzie nieobecności AI Mety w UE. Dlatego suwerenność cyfrowa musi być budowana w sposób pragmatyczny, tak aby nie stracić na konkurencyjności gospodarki UE oraz nie ponosić olbrzymich kosztów i nie zostać w tyle.

Poniższy raport koncentruje się na przedstawieniu optymalnej i pragmatycznej „środkowej drogi”, która będzie operacyjna dla Unii Europejskiej i jej członków. W raporcie przedstawiono czym jest suwerenność cyfrowa oraz jak jest rozumiana, a szczególny nacisk położono na zdefiniowanie pragmatycznej suwerenności oraz przedstawienie charakterystycznych jej cech. Raport charakteryzuje również jak tę koncepcję postrzega Unia Europejska i jakie działania podejmuje w celu jej osiągnięcia. Na końcu zawarto główne wnioski i rekomendacje dotyczące osiągnięcia suwerenności cyfrowej.

1 <https://wydarzenia.interia.pl/zagranica/news-wydal-nakaz-aresztowania-netanjahu-jego-zycie-zmienilo-sie-w,nld,22456967>

2 <https://cepa.org/article/digital-sovereignty-can-europe-afford-it/>

1. Suwerenność cyfrowa

Koncepcja suwerenności cyfrowej kojarzy się często z tendencjami państw autorytarnych takich jak Chiny, Rosja i Iran, które chciałyby sprawować całkowitą dominację nad obszarem technologicznym, a przede wszystkim w pełni kontrolować obieg informacji. Ten charakter suwerenności cyfrowej znajduje odzwierciedlenie w rosyjskim Runecie czyli kontrolowanym przez państwo zamkniętym Internecie³ czy chińskim Wirtualnym Wielkim Murze. Chiny rozwijają własne aplikacje takie jak WeChat, które można określić mianem aplikacji do wszystkiego, ale również zastępują popularne media społecznościowe takie jak Facebook, X czy Instagram własnymi chińskimi rozwiązaniami⁴. To przykład skrajnej wersji suwerenności cyfrowej, która jednak nie bazuje w 100% na rodzimych rozwiązaniach, ponieważ zarówno Chiny i Rosja nadal używają systemów Microsoft Windows.

Mamy też inne rozumienie suwerenności cyfrowej, którą można przedstawić jako ideę kontroli tego co cyfrowe w warstwie fizycznej (zasoby, infrastruktura, urządzenia), warstwie kodu (standardy, zasady, design) oraz w warstwie informacji (treści, dane). Kontrolę rozumie się tutaj jako zdolność wpływu i ograniczania produkcji, projektowania oraz wykorzystania wyników technologii cyfrowych. Tak rozumiana suwerenność nie powinna być mylona z autarkią bądź próbą faktycznego robienia tego wszystkiego we wszystkich kluczowych technologiach wspomagających i ich komponentach⁵.

Cyfrowa suwerenność Unii Europejskiej

Przez długi okres zwolennicy globalizacji przekonywali, że kapitał i technologie nie mają narodowości. W trzeciej dekadzie XXI wieku widać, że technologia podobnie jak kapitał ma narodowość, a koncepcje globalistycznych hurraoptymistów nie spełniły się. Dynamiczna sytuacja geopolityczna, która stale ewoluje w zakresie stosunków na linii Unia Europejska – Chiny i UE - Stany Zjednoczone (a więc główni dostawcy technologii), powoduje, że koncepcja suwerenności cyfrowej⁶ powraca do szerokiej dyskusji w ramach UE. Budowanie oparcia w unijnej regulacji, może być odbierane jako krok nieprzyjazny wobec Stanów Zjednoczonych, szczególnie biorąc pod uwagę, że obecna administracja prezydenta Trumpa jest dość krytyczna wobec Starego Kontynentu.

3 <https://cyberdefence24.pl/technologie/runet-rosja-przetestowala-odlaczenie-od-miedzynarodowego-internetu>

4 https://demagog.org.pl/analizy_i_raporty/wirtualny-wielki-mur-jak-partia-ksztaltuje-chinski-internet/

5 https://www.politykainsight.pl/_resource/multimedium/20393469, s 12/

6 Suwerenność cyfrowa to koncepcja odnosząca się do zdolności państwa, organizacji, jednostki do samodzielnego kontrolowania swoich zasobów cyfrowych, w tym danych, infrastruktury IT, technologii i usług online. Zakłada niezależność od zewnętrznych wpływów, szczególnie BigTechów oraz ochronę przed inwigilacją, cyberatakami czy uzależnieniem od zagranicznych dostawców.

Bruksela obawia się o swoje bezpieczeństwo, ale również traktuje suwerenność cyfrową jako sposób UE na zwiększenie roli na międzynarodowych rynkach technologicznych oraz ochronę konkurencyjności własnej gospodarki. Jest to szczególnie istotne w czasach kryzysu globalizacji oraz światowego handlu.

To nie pierwszy raz, kiedy Unia Europejska przywołuje koncepcję suwerenności technologicznej. W 2016 roku komisarz Viviane Reding w swym eseju podkreśliła znaczenie suwerenności cyfrowej Europy⁷. Była to niejako odpowiedź na rozbudowaną wówczas inwigilację Stanów Zjednoczonych. Wykradzione przez analityka amerykańskiego wywiadu Edwarda Snowdena dokumenty, pokazywały jak amerykańska technologia wykorzystywana jest przez służby do szpiegowania - również swoich sojuszników z NATO. Ideę cyfrowej suwerenności kontynuowała szefowa Komisji Europejskiej Ursula von der Leyen, w trakcie trwania swojej pierwszej kadencji, rozpoczętej w 2019 roku. W tym czasie, koncepcja ta pojawiała się wielokrotnie zarówno w dokumentach UE i wypowiedziach decydentów. Pandemia COVID-19 wymusiła masowe wdrożenie narzędzi cyfrowych do monitorowania procesów związanych z jej zwalczaniem, pracy zdalnej czy edukacji, ale również pokazała zależność Unii Europejskiej od zagranicznych technologii, co prowadziło do intensyfikacji dyskusji na temat suwerenności cyfrowej⁸. W 2020 roku szefowa Komisji w eseju przedstawiła swoją wizję technosuwerenności, jako możliwość posiadania zdolności technologicznych oraz swobodę wyboru technologii, w tym w ramach współpracy międzynarodowej. W podobnym tonie wypowiadali się przywódcy Francji i Niemiec w 2025 roku podczas Szczytu Europejskiej Suwerenności w Berlinie⁹. Ponadto analiza dokumentów oraz opracowań akademickich na temat suwerenności cyfrowej UE, podkreśla co do zasady skupienie się na dwóch głównych filarach – własnych kompetencjach i kształtowaniu relacji z zewnętrznymi podmiotami¹⁰. Jak widać koncepcja suwerenności cyfrowej UE jest różna od koncepcji całkowitej autarkii.

W drugiej kadencji Ursuli von der Leyen, koncepcja suwerenności cyfrowej jest rozwijana w oparciu o szereg dokumentów strategicznych. Pierwszym z nich było wyznaczenie celów dotyczących transformacji cyfrowej na lata 2020-2025 w ramach dokumentu „Kształtowanie cyfrowej przyszłości Europy”, który wyznaczał trzy główne cele:

- ▶ Technologia, która służy ludziom
- ▶ Sprawiedliwa i konkurencyjna gospodarka
- ▶ Otwarte, demokratyczne i zrównoważone społeczeństwo

Cele te wskazują na konieczność osiągnięcia niezależności i tworzenie własnych rozwiązań cyfrowych, a nie opieraniu się na technologiach zaprojektowanych przez kogoś innego. Kluczem mają być tu dane i ich ponowne wykorzystanie oraz fakt, że wszystkie firmy powinny konkurować na równych zasadach¹¹.

7 Viviane Reding, 'Digital Sovereignty: Europe at a Crossroads' (2016) <https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europ>

8 <https://cyberpolicy.nask.pl/pandemia-covid-19-a-kwestie-zarzadzania-internetem/>

9 <https://www.bundesregierung.de/breg-de/aktuelles/summit-on-european-digital-sovereignty-delivers-landmark-commitments-for-a-more-competitive-and-sovereign-europe-2394368>

10 https://www.politykainsight.pl/_resource/multimedia/20393469

11 <https://www.gov.pl/web/cyfryzacja/cyfrowa-przyszlosc-europy---priorytety-na-najblizsze-5-lat>

Rok później KE opublikowała komunikat „Cyfrowy Kompas na rok 2030: europejska droga w cyfrowej dekadzie”, który przedstawia wizję i cele transformacji cyfrowej Europy do 2030 roku. W ramach tego dokumentu zaplanowano zapewnienie strategicznej cyfrowej suwerenności Unii z zachowaniem otwartości, w szczególności poprzez bezpieczną i dostępną infrastrukturę cyfrową i infrastrukturę danych, zdolną do efektywnego przechowywania, przesyłania i przetwarzania bardzo dużych ilości informacji. Ma to umożliwić inne osiągnięcia technologiczne, wspierając jednocześnie konkurencyjność, zrównoważony przemysł i gospodarkę Unii, zwłaszcza sektor Małych i Średnich Przedsiębiorstw oraz wzmocnić odporność unijnych łańcuchów dostaw, a także sprzyjać ekosystemowi start-upów i sprawnemu funkcjonowaniu europejskich innowacji cyfrowych. Jednym z narzędzi za pomocą których UE ma zamiar osiągać cyfrową suwerenność jest promowanie unijnego cyfrowego otoczenia regulacyjnego, które ma wspierać zdolności przedsiębiorstw w UE. W celu monitorowania postępów odnoszących się do celów ogólnych i cyfrowych, KE zastosowała źródła danych DESI (Indeks gospodarki cyfrowej i społeczeństwa cyfrowego) oraz KPIs (Key Performance Indicators). Sprawozdanie ma być przesyłane corocznie do Parlamentu Europejskiego i Rady¹².

Cyfrowy Kompas koncentruje się na czterech obszarach: społeczeństwo, infrastruktura, biznes oraz usługi publiczne. KE planuje, aby do 2030 roku 80% Europejczyków posiadało przynajmniej podstawowe kompetencje cyfrowe (aktualnie wskaźnik ten wynosi 56%). Liczba ekspertów z branży teleinformatycznej ma wzrosnąć do 20 milionów (obecnie jest to 7,8 miliona). Najważniejszym projektem infrastrukturalnym jest sieć 5G, która ma pokrywać wszystkie obszary zaludnione. Planuje się również podwojenie unijnego udziału w produkcji półprzewodników z 10% do 20% wartości rynku. UE zamierza również rozwijać inicjatywy pozwalające firmom na ograniczenie zależności od pozaeuropejskich usługodawców w obszarze przechowywania danych. W Kompasie zaplanowano także budowę pierwszego europejskiego komputera kwantowego. UE ma też plany dotyczące używania chmury obliczeniowej, AI i BIG DATA przez europejskich przedsiębiorców, do poziomu 75%. Zinformatyzowane mają być usługi publiczne, a 100% najważniejszych usług w całej UE ma być scyfryzowanych (obecnie to 75% dla obywateli i 84% dla biznesu) przy wskaźniku 80% Europejczyków korzystających z cyfrowego dowodu tożsamości (eIDAS)¹³. Plany są bardzo ambitne i stanowią szansę dla rozwoju europejskiego sektora IT, a tym samym budowania suwerenności cyfrowej.

W rozważaniach strategiczno-koncepcyjnych nie można pominąć raportu byłego szefa Europejskiego Banku Centralnego Mario Draghiego, który przedstawił raport na temat konkurencyjności UE. Jednym z czynników, który spowodował, że UE znalazła się w obecnym stanie, było niewykorzystanie pierwszej fali cyfryzacji. Ponadto problemem są dysproporcje finansowe w zakresie technologicznym. Firmy z UE otrzymują zaledwie 6% całkowitego finansowania przeznaczonego na rozwój projektów z zakresu sztucznej inteligencji. Większość tych środków trafia do firm z siedzibą w USA, gdzie lokowane jest aż 61% globalnych inwestycji, a 17% do Chin, co wyraźnie pokazuje niewielką rolę UE

¹² <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52021DC0118>

¹³ https://pism.pl/publikacje/Cyfrowa_dekada_UE_cele_i_wyzwania

w poziomie wsparcia finansowego¹⁴. Inne przyczyny, które spowodowały, że UE straciła pozycję z lat 90. to nadmierne regulacje i biurokracja. Z jednej strony chronią one konsumentów, ale często spowalniają rozwój firm technologicznych, prowadząc do ograniczenia rozmiaru przedsiębiorstw, komplikując procesy innowacyjne czy zwiększając koszty operacyjne¹⁵. Kolejnym problemem są niskie nakłady na badania i rozwój oraz brak kapitału venture capital na dużą skalę, co sprawia, że europejskie start-upy rzadko rosną do poziomu gigantów¹⁶. Ponadto fakt, że UE składa się z 27 państw o różnych regulacjach, językach czy odmiennej kulturze biznesowej, utrudnia skalowanie innowacji. Co więcej, Europa ma problem z adaptacją technologii cyfrowych w gospodarce, co obniża produktywność¹⁷.

W swoim raporcie Draghi zaprezentował szeroką koncepcję wzmocnienia cyfrowej konkurencyjności Unii Europejskiej. Unaoczniał skalę uzależnienia od zagranicznych technologii: w przypadku rynku chmury obliczeniowej jest to 80%, a urządzeń mobilnych prawie 100%. Udział podmiotów z UE w globalnym rynku przewodników to obecnie tylko 10,5 proc¹⁸.

Draghi zaproponował również szereg inicjatyw mających na celu zmianę tej sytuacji i wzmocnienie konkurencyjności UE. W ramach swoich rozważań, zaproponował konsolidację operatorów telekomunikacyjnych, tak by stworzyć podmioty o skali mogącej konkurować z globalnymi gigantami. Innym pomysłem jest wprowadzenie opłat od dostawców treści internetowych dla operatorów za korzystanie z infrastruktury. Draghi sugeruje, że łączna suma rocznych inwestycji związanych z transformacją energetyczną i cyfrową powinna oscylować w granicach 750-800 miliardów euro rocznie, aby pobudzić konkurencyjność UE. Priorytet w finansowaniu powinny otrzymać trzy sektory:

- ▶ infrastruktura szerokopasmowego Internetu wraz ze sprzętem i oprogramowaniem,
- ▶ rozwój zdolności obliczeniowych oraz technologii związanych ze sztuczną inteligencją,
- ▶ produkcja i innowacyjność w obszarze półprzewodników¹⁹.

Nie pierwszy raz Unia Europejska promuje koncepcję suwerenności cyfrowej. Tym razem jednak za polityczno-strategicznymi dokumentami podążają decyzje podjęte przez europejski biznes. Pod koniec 2025 perła w koronie europejskiego przemysłu - Airbus - zadeklarował, że planuje ograniczyć współpracę z Google i Microsoft w obszarze usług biurowych i chmurowych, motywując to kwestiami bezpieczeństwa. Jednocześnie jednak podkreślił, że nie ma pewności czy uda się znaleźć europejskiego dostawcę, który będzie w stanie spełnić ich wymagania. Nie oznacza to oczywiście całkowitej rezygnacji z usług Google, które w mniej krytycznych obszarach firmy będą nadal używane.

Firma przygotowuje się do przeniesienia strategicznych systemów zarządzania przedsiębiorstwem i do lata 2026 ma zamiar wybrać europejskiego dostawcę usług chmurowych,

14 <https://wei.org.pl/2025/aktualnosci/cezary-bachanski/europejska-suwerennosc-cyfrowa-czyli-jak-unia-europejska-chce-zwiekszyc-swoje-swiatowe-znaczenie-w-technologiach-cyfrowych/>

15 <https://www.gisreportsonline.com/r/innovation-regulation>

16 <https://itif.org/publications/2025/07/14/europes-innovation-lethargy-lesson-of-what-not-to-do/>

17 <https://www.realinstitutoelcano.org/en/analyses/competitiveness-the-widening-gap-between-the-eu-and-the-us/>

18 Omówienie raportu Dragiego <https://wei.org.pl/2025/aktualnosci/cezary-bachanski/europejska-suwerennosc-cyfrowa-czyli-jak-unia-europejska-chce-zwiekszyc-swoje-swiatowe-znaczenie-w-technologiach-cyfrowych/>

19 Omówienie raportu Dragiego <https://wei.org.pl/2025/aktualnosci/cezary-bachanski/europejska-suwerennosc-cyfrowa-czyli-jak-unia-europejska-chce-zwiekszyc-swoje-swiatowe-znaczenie-w-technologiach-cyfrowych/>

który przejmie obsługę tych systemów. Wartość kontraktu może przekroczyć 50 milionów euro, co powoduje, że będzie to największy projekt chmurowy realizowany obecnie w Europie. Decyzja ta związana jest z amerykańską ustawą Cloud Act, która umożliwia władzom USA możliwość żądania dostępu do danych przechowywanych przez amerykańskie firmy, nawet jeżeli znajdują się one poza granicami państwa. Na poziomie technicznym najważniejszym zagadnieniem pozostaje kwestia dostępu do kluczy szyfrujących dane. Dostawcy usług w chmurze stosują w tym zakresie różne modele - w części rozwiązań operator posiada dostęp do kluczy szyfrujących dane klientów, w innych odpowiedzialność za ich zarządzanie spoczywa wyłącznie po stronie właściciela danych. W przypadku np. Google Cloud dostawca nie ma technicznej możliwości dostępu do kluczy szyfrujących, ponieważ pozostają one pod wyłączną kontrolą właściciela danych. Biorąc pod uwagę, że Airbus to główny konkurent Boeinga, mocno wspieranego przez amerykański rząd, obawy europejskiego giganta mogą być uzasadnione, w szczególności, jeżeli weźmie się pod uwagę, że do władzy doszła administracja prezydenta Trumpa, która od początku wykazuje negatywną postawę względem Unii Europejskiej.

Nie tylko jednak ponowne dojście do władzy Donalda Trumpa wzmocniło sceptycyzm wobec amerykańskich produktów. W 2024 Microsoft przyznał przed francuskim sądem, że nie jest w stanie zagwarantować pełnej suwerenności danych europejskich klientów²⁰. Ruch Airbasa będzie z pewnością obserwowany przez inne europejskiej firmy - mówimy w końcu o gigancie zatrudniającym ponad 157 tys. osób i generujący dziesiątki miliardów euro. Pytanie czy Airbus znajdzie odpowiedniego europejskiego dostawcę - co z pewnością będzie realnym testem czy europejska suwerenność cyfrowa może istnieć poza dokumentami strategicznymi i politycznymi deklaracjami. Udana migracja do europejskich usług chmurowych, może stanowić punkt zwrotny w budowaniu pragmatycznej suwerenności cyfrowej i być sygnałem dla innych firm europejskich, że możliwe jest funkcjonowanie bez amerykańskich dostawców chmurowych.

20 https://ithardware.pl/aktualnosci/airbus_google_europa_usa-47461.html

2. Pragmatyczne podejście do koncepcji cyfrowej suwerenności

Cyfrowa suwerenność zbyt często jest teoretycznym konstruktem, który stawia idealistyczne cele pełnej kontroli w obszarze technologii. Tego nie da się zrealizować obecnie - nawet Stany Zjednoczone i Chiny, które są na tym polu potentatami, współdzielą wiele rozwiązań. Dlatego konieczne jest przyjęcie „środkowej drogi” – pragmatycznego modelu, który nie idzie w kierunku pełnej nacjonalizacji, a w przypadku Unii Europejskiej europeizacji rozwiązań, ale też nie porzuca całkowicie suwerenności cyfrowej. Dlatego konieczne jest pragmatyczne podejście do cyfrowej suwerenności chroniące swoje najważniejsze zasoby, nie tracące na konkurencyjności, ale zachowujące przy tym realistyczne cele do zrealizowania.

W pragmatycznym podejściu, model ten odchodzi od idealistycznej wizji całkowitej izolacji i samowystarczalności skupiając się na praktycznych, elastycznych rozwiązaniach, które łączą bezpieczeństwo z efektywnością ekonomiczną i innowacyjnością. Zamiast odgradzać od świata i budować mur wokół technologii, polityka ta bazuje na współpracy międzynarodowej i najlepszym wykorzystaniu dostępnych narzędzi, jednocześnie minimalizując ryzyko.

Kluczowe cechy, którymi powinien charakteryzować się pragmatyczny model suwerenności cyfrowej to:

Wolność wyboru i interoperacyjność. Suwerenność w tym kontekście powinna zaczynać się od możliwości swobodnego wyboru technologii bez uzależniania się od jednego dostawcy (tzw. vendor lock-in). Uzależnienie od jednego dostawcy niezależnie od jego kraju pochodzenia, nawet jeśli pochodzi z terenu Wspólnoty nie jest niczym dobrym. Jeden incydent, awaria u dostawcy usług może prowadzić do gigantycznych wzrostów kosztów lub opóźnień w dostawach, a nawet przerwy w dostarczanej usłudze. Uzależnienie od jednego dostawcy może powodować ograniczenie elastyczności oraz zmiany kierunku działania, a w najgorszym razie to klient musi dostosować się do warunków dyktowanych przez dostawcę, co może utrudniać rozwój firmy. Ryzykuje również przepłaceniem za usługi czy ograniczeniem innowacyjności²¹. Kluczowe wydaje się tutaj wdrażanie otwartych standardów, które pozwalają łączyć rozwiązania różnych firm, elastycznie reagować na zmiany i podnosić bezpieczeństwo systemów. Taki model unika izolacji rynku, uznając, że globalna współpraca jest niezbędna dla innowacji. Przykładowo administracja publiczna może preferować systemy modułowe, umożliwiające łatwą migrację danych²².

21 <https://www.e-point.pl/blog/vendor-lock-in-w-instytucjach-finansowych>, <https://www.advox.pl/blog/w-technologicznej-pulapce-czym-jest-vendor-lock-in-i-jak-go-uniknac>, <https://www.hostersi.pl/blog/vendor-lock-in-czyli-jak-sobie-radziec-z-zalezno-scia-od-dostawcy-uslug-chmurowych/#:~:text=Co%20to%20jest%20Vendor%20Lock,utrudnia%20migracj%C4%99%20do%20innej%20platformy>.

22 <https://cyfrowapolska.org/suwerennosc-cyfrowa-zaczyna-sie-od-wolnosci-wyboru-technologii-nie-od-izolacji-rynku-stanowisko/>

Konkretne rozwiązania zamiast ideałów. Zamiast dążyć do pełnej samowystarczalności (co jest często nierealne i kosztowne), model pragmatyczny powinien się skupiać na praktycznych decyzjach jak rozwój własnego oprogramowania, które będzie używane w administracji rządowej czy infrastrukturze krytycznej. We Francji istnieją już takie aplikacje jak Tchap czy Olvid, które są używane do oficjalnej komunikacji, jednocześnie pracownicy rządowi mają zakaz używania innych komunikatorów do komunikacji służbowej²³. W tym samym czasie Komisja Europejska rekomendowała korzystanie z aplikacji Signal, która uchodzi za bezpieczną, choć nie jest rozwiązaniem europejskim, lecz pochodzi ze Stanów Zjednoczonych²⁴. Co stałoby na przeszkodzie aby rozszerzyć francuskie rozwiązanie na własne instytucje?

Dostosowana ochrona danych i międzynarodowe normy są niezbędne. Tworzenie norm prawnych przez UE ma sens i przykład RODO pokazuje, że może okazać się sukcesem. UE jest na tyle dużym rynkiem, że dostawcy usług cyfrowych zaadaptują się do zmian. Państwa i UE powinny wykorzystać najlepsze technologie dostępne na rynku jednocześnie budując kontrolę nad kluczowymi zasobami jak np. danymi używanymi przez kluczowe instytucje takie jak np. siły zbrojne. Przykładem tutaj jest postawa Szwajcarii, która wprowadziła do UE nie należy, ale odmówiła kontraktu amerykańskiemu przedsiębiorstwu Palantir powołując się na zwiększenie zależności od amerykańskiego dostawcy technologii oraz ryzyko potencjalnej utraty kontroli danych i suwerenności narodowej. Inaczej zachowała się Polska podpisując z Palantirem list intencyjny na dostawy produktów dla wojska²⁵ czy Wielka Brytania i Niemcy decydując się na współpracę z Google²⁶. W ramach budowania suwerenności cyfrowej, konieczne jest jasne wyodrębnienie sektorów, gdzie współpraca i wymiana informacji z zagranicznymi koncernami będzie odbywała się na specjalnych zasadach, ograniczając możliwość wycieku informacji na zewnątrz. Siły zbrojne z pewnością powinny należeć do tych kluczowych sektorów. Takie rozwiązanie przyjęła Agencja Komunikacji i Informacji NATO (NCIA) podejmując współpracę z Google wprowadzając wersję chmury GDC air-gapped, czyli chmury, która działa bez połączenia z Internetem w środowisku suwerennym i odizolowanym, co pozwala NCIA korzystać z rozwiązań opartych na sztucznej inteligencji i narzędziach bez ryzyka wycieku danych, co umożliwia przetwarzanie wrażliwych danych w bezpiecznym środowisku²⁷. Suwerenność to nie budowa własnych centrów danych, ale inteligentne wybory zapewniające efektywność i konkurencyjność, a przykładem tego może być podejmowanie współpracy z zagranicznymi firmami na specjalnych zasadach, do których muszą się one dostosować. Należy też ułatwić współdzielenie usług chmurowych na wspólnych zasadach między państwami²⁸.

Lokalna infrastruktura i kontrola danych. Model ten opiera się na inwestycjach w lokalne zasoby, takie jak centra danych, umożliwiające przechowywanie danych na terytorium

23 <https://www.bleepingcomputer.com/news/security/french-government-recommends-against-using-foreign-chat-apps/#:~:text=Prime%20Minister%20of%20France%20%C3%89lisabeth,to%20Le%20Point%20published%20excerpts>.

24 <https://aboutsignal.com/news/european-commission-internally-recommends-signal-with-disappearing-messages/>

25 <https://cyberdefence24.pl/cyberbezpieczenstwo/szwajcarska-armia-rezygnuje-z-palantira-zbyt-duze-ryzyko>

26 <https://www.gov.uk/government/news/security-delivered-for-working-people-as-uk-us-ties-strengthened-with-new-google-cloud-partnership-for-classified-information-sharing>

27 <https://cyberdefence24.pl/cyberbezpieczenstwo/wielomilionowa-umowa-nato-z-google-cloud>

28 <https://www.pb.pl/prezes-sap-suwerennosc-cyfrowa-dotyczy-konkretnych-rozwiazan-a-nie-teoretycznych-idealow-opinia-1251023>

danego kraju. Takie podejście pozwala spełnić wymogi regulacyjne bez konieczności rezygnacji z globalnych rozwiązań technologicznych ani hamowania innowacji. Należy jednak podkreślić, że budowa centrów danych całkowicie pozbawionych komponentów pochodzących ze Stanów Zjednoczonych lub Chin jest w praktyce niemożliwa. Pokazuje to skalę globalnych zależności w sektorze technologicznym i jasno wskazuje, że pełna autarkia w tym obszarze pozostaje nieosiągalna.

Otwarte ryzyko i derisking. Model ten zakłada systematyczną ocenę zagrożeń geopolitycznych, jak i związanych z cyberbezpieczeństwem oraz wzmacnianie odporności w sposób racjonalny, bez ulegania nadmiernym obawom. Koncepcja otwartej autonomii strategicznej łączy podejście deriskingowe, polegające na ograniczaniu krytycznych zależności, z utrzymaniem współpracy z partnerami zewnętrznymi.

Współpraca i uczenie się. Pragmatyzm wymaga wymiany doświadczeń między różnymi państwami na całym świecie.

Edukacja i wysoce wykwalifikowani eksperci. Ważnym elementem osiągnięcia suwerenności cyfrowej są inwestycje w krajową edukację, szkolenia i badania w dziedzinie nowoczesnych technologii chmury obliczeniowej. Fundamentem cyfrowej suwerenności są zarówno świadome i odpowiedzialne społeczeństwo, jak i eksperci rozwijający oraz zabezpieczający nowe technologie.

Osiągalnym minimum, mającym jednak fundamentalne znaczenie dla suwerenności cyfrowej, powinny być:

- ▶ możliwość samodzielnego administrowania danymi,
- ▶ tworzenie oprogramowania niezbędnego do funkcjonowania państwa i infrastruktury krytycznej,
- ▶ zapobieganie zagrożeniom w cyberprzestrzeni.

Big Techy, odpowiadając na debatę dotyczącą cyfrowej suwerenności, zaczęły proponować własne rozwiązania. Jednym z pierwszych podmiotów, który wystąpił z taką inicjatywą, był Microsoft. „Korporacja rozumie suwerenność cyfrową jako zapewnienie klientom pełnej kontroli nad danymi, infrastrukturą i zgodnością z lokalnym prawem, przy jednoczesnym korzystaniu z globalnych innowacji technologicznych”²⁹.

Pierwszy filar strategii stanowi infrastruktura — przede wszystkim lokalnie zlokalizowane centra danych. Microsoft odpowiada na to zapotrzebowanie, tworząc np. centra przetwarzania danych w okolicach Warszawy. Drugim filarem miała być tzw. EU Data Boundary — zobowiązanie wykraczające poza wymogi RODO i zakładające niedopuszczanie do transferu danych poza Unię Europejską. Trzecią kwestią jest kontrola techniczna — klienci oczekują gwarancji, że Microsoft nie ma możliwości uzyskania dostępu do danych bez ich wyraźnej zgody. Dlatego opracowano zestaw narzędzi, które realnie przekazują kontrolę w ręce użytkowników. Obejmują one m.in. mechanizmy umożliwiające przetwarzanie danych w postaci zaszyfrowanej bez konieczności ich odszyfrowywania (Confidential

29 <https://spidersweb.pl/2025/12/suwerennosc-cyfrowa-europa-microsoft.html>

Computing), system Customer Lockbox wymagający każdorazowej, jawnej zgody klienta na dostęp do danych, a także możliwość przechowywania kluczy szyfrowania poza chmurą Microsoft Azure — u zaufanych partnerów. Czwartym elementem jest odporność, rozumiana jako budowa systemu umożliwiającego odtwarzanie danych z różnych regionów Europy, nawet w przypadku awarii lub sytuacji kryzysowych. Microsoft zaproponował również koncepcję Digital Resilience Commitment, czyli zobowiązanie do cyfrowej odporności. Zakłada ono, że w przypadku żądania zaprzestania świadczenia usług firma zobowiązuje się dochodzić swoich racji na drodze sądowej, aby usługi pozostały dostępne dla klientów. Ponadto kod źródłowy ma być przechowywany w neutralnej Szwajcarii³⁰. Oferta korporacji mogłaby wyglądać interesująco, gdyby nie jeden fakt. Główny zarzut, który pojawia się odnośnie do tej koncepcji to zeznanie dyrektora Microsoftu, który przed francuskim sądem przyznał, że nie uchroni danych Europejczyków przed amerykańskimi sądami jeśli o nie zapytają³¹. Biorąc pod uwagę obecną politykę administracji USA, która nawet w głównym dokumencie strategicznym jakim jest Narodowa Strategia Bezpieczeństwa, mocno akcentowała antyeuropejskie wartości, słowa francuskiego oddziału Microsoftu nabierają nowego znaczenia³².

Microsoft nie jest jedynym BigTechem, który swoimi rozwiązaniami technologicznymi zamierza wyjść naprzeciw suwerenności cyfrowej. Amazon również proponuje Europejską Suwerenną Chmurę, gdzie wszystkie komponenty miałyby znajdować się w Unii Europejskiej, a infrastruktura miałaby być zarządzana przez jednostkę zlokalizowaną w Niemczech i podlegającą europejskiemu prawu. Została ona poddana audytowi, a Niemiecki Federalny Urząd Bezpieczeństwa Informacji przydzielił jej certyfikat bezpieczeństwa C5³³. Krytycy podkreślają, że rozwiązanie proponowane przez Amazon nie gwarantuje, iż dane nie mogą zostać udostępnione organom amerykańskim na mocy US CLOUD Act³⁴.

Jak już wspomniano wcześniej w raporcie, na poziomie technicznym, bardzo ważnym aspektem dotyczącym dyskusji o suwerenności i kontroli nad dostępem do danych jest kwestia zarządzania kluczami szyfrującymi. Wszyscy globalni dostawcy usług chmurowych, tzw. hyperscalerzy, przechowują wyłącznie dane zaszyfrowane. Różnice pojawiają się natomiast w zakresie zarządzania kluczami szyfrującymi. Google Cloud daje pełną kontrolę nad kluczami swoim klientom — właścicielom danych, podczas gdy u innych dostawców zarządzanie kluczami jest współdzielone między właściciela danych a dostawcę infrastruktury. Istotne różnice mogą występować również w procedurach odpowiadania na wnioski służb o dostęp do danych oraz w możliwościach przesyłania danych między różnymi dostawcami.

Jeszcze lepszą ochronę zapewnia przed konsekwencjami US CLOUD Act zapewnia S3NS, czyli spółka Joint Venture pomiędzy Thalesem (51%) a Google (49%). Jest to lokalna, izolowana chmura oparta na technologii Google Cloud, do której pracownicy Google nie mają dostępu. Rozwiązanie to jest adresowane do branż przetwarzających wrażliwe informacje

30 <https://spidersweb.pl/2025/12/suwerennosc-cyfrowa-europa-microsoft.html>

31 <https://wyborcza.biz/biznes/7,177150,32177247,microsoft-przyznał-nie-uchronimy-danych-europejczykow-przed.html?disable-Redirects=true>

32 <https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf>

33 <https://aws.amazon.com/blogs/aws/opening-the-aws-european-sovereign-cloud/>

34 <https://www.trendingtopics.eu/amazon-new-european-sovereign-cloud-cant-rule-out-us-data-access/>

z sektora bezpieczeństwa³⁵. O bezpieczeństwie i prywatności tak przetwarzanych danych świadczy fakt, że otrzymała ona certyfikat najwyższego stopnia SecNumCloud 3.2 od francuskiej agencji cyberbezpieczeństwa ANSSI. Postrzegany jest on jako najtrudniejszy do uzyskania, a jego celem jest ochrona przed eksterytorialnymi żądaniami Stanów Zjednoczonych i Chin mającymi zmuszać korporacje do ujawniania wrażliwych danych ich klientów³⁶. Wydaje się, że to podejście najlepiej wpisuje się w projektowaną europejską koncepcję cyfrowej suwerenności — umożliwia korzystanie z międzynarodowych dostawców przy zachowaniu wymaganego poziomu kontroli i bezpieczeństwa danych.

Omawiając rozwiązania hyperscalerów z zakresu suwerenności warto też zwrócić uwagę na kwestię związaną ze zjawiskiem vendor lock-inu oraz przesyłania danych między dostawcami chmury. Google Cloud wydaje się dostrzegać potrzebę rynku w zakresie zwiększenia swobody właścicieli danych w podejmowaniu decyzji o tym, gdzie ich dane są przechowywane oraz stawiania na rozwiązania wielochmurowe (ang. multi-cloud). W 2025 roku jako pierwszy hyperscaler, Google Cloud ogłosiło inicjatywę Data Transfer Essentials, która zapewnia klientom z UE i Wielkiej Brytanii przesyłanie danych do innych dostawców bez dodatkowych opłat.

Zagrożenia związane z osiągnięciem suwerenności cyfrowej

Budowanie cyfrowej suwerenności może wiązać się z szeregiem zagrożeń, zwłaszcza jeśli proces ten jest realizowany w sposób nieumiejętny. Do zagrożeń związanych z budową cyfrowej suwerenności należą kwestie ekonomiczne, w tym wyższe koszty wynikające z konieczności tworzenia lokalnej infrastruktury. Kolejnym ryzykiem jest potencjalna izolacja od globalnych trendów, co może spowalniać rozwój, a ograniczona możliwość wyboru technologii może dodatkowo osłabiać odporność na zagrożenia w cyberprzestrzeni. Nie zawsze lokalna kontrola przekłada się na wyższy poziom ochrony — słabsze systemy mogą stać się celem częstszych ataków. Ponadto sprawowanie lokalnej kontroli może ograniczać dostęp do globalnego obiegu informacji o zagrożeniach w cyberprzestrzeni, co utrudnia skuteczne zabezpieczenie zasobów. Suwerenność cyfrowa niesie ze sobą również ryzyko pogłębiającej się fragmentacji Internetu, co może utrudniać współpracę międzynarodową oraz handel, negatywnie wpływając na wzrost gospodarczy.

Często w dyskusjach nad tworzeniem suwerenności cyfrowej powraca koncepcja odrzucenia pewnych rozwiązań z góry, ze względu chociażby na kraj pochodzenia. Niestety może to prowadzić do tzw. vendor lock-in czyli uzależnienia od jednego dostawcy, którego ewentualna zmiana jest niezwykle trudna do przeprowadzenia. Zagrożenia związane z vendor lock-in można podzielić na wiele obszarów. Ekonomiczne wyzwania wiążą się z wymaganym przeniesieniem danych, co generuje koszty wynikające z integracji nowych rozwiązań oraz szkoleniem nowych pracowników. W niektórych obszarach jak np. w handlu elektronicznym może to wiązać się z dodatkowymi wydatkami na pozyskanie modułów

35 <https://cloud.google.com/blog/products/identity-security/google-advances-sovereignty-choice-and-security-in-the-cloud>

36 <https://www.euractiv.com/news/google-backed-cloud-wins-frances-strongest-sovereignty-certification/>

i wsparcia czy utrudniać integrację z innymi systemami³⁷. Drugi problem związany jest z kwestiami operacyjnymi, czyli brakiem elastyczności i trudnościami z integracją. Uzależnienie od lokalnych rozwiązań zmniejsza zdolność szybkiej adaptacji do zmian rynkowych lub wdrażania nowych narzędzi, co może spowalniać rozwój biznesu³⁸.

37 <https://e-handelwpraktyce.pl/slownik/vendor-lock-in-uzaleznienie-od-jednego-dostawcy-technologiei>

38 <https://www.e-point.pl/blog/vendor-lock-in-w-instytucjach-finansowych>

3. Unia Europejska na drodze do realizacji pragmatycznej suwerenności

Unia Europejska, dążąc do uzyskania cyfrowej suwerenności, stosuje podejście dwutorowe. Z jednej strony poprzez instrumenty finansowe próbuje stymulować rozwój europejskich rozwiązań technologicznych, które mogą stać się alternatywą w stosunku do Chin i Stanów Zjednoczonych. Drugim podejściem jest szeroko pojęta legislacja, która ma doprowadzić do sytuacji, w której globalni dostawcy technologii dostosują swoje rozwiązania do wymagań unijnych. Analiza strategicznych dokumentów UE i metod finansowania pozwala na wyróżnienie następujących kluczowych obszarów:

- ▶ kontrola i możliwość samodzielnego administrowania danymi,
- ▶ rozwój sztucznej inteligencji,
- ▶ półprzewodniki,
- ▶ technologia chmurowa.

Finansowanie

Kluczową rolę w zwiększaniu zdolności UE do osiągnięcia cyfrowej suwerenności odgrywa Wieloletnie Ramy Finansowe. W założeniach na lata 2028–2034 przewidziano przeznaczenie na ten cel ponad 600 miliardów euro. Planuje się utworzenie Europejskiego Funduszu Konkurencyjności o wartości przekraczającej 400 miliardów euro. Ponadto w ramach Programu Horyzont Europa zostanie przeznaczone 175 miliardów euro na finansowanie innowacji, w tym projektów związanych z AI, obliczeniami kwantowymi i suwerennością danych. Dodatkowe nakłady finansowe na budowanie suwerenności są również zaplanowane w ramach Instrumentu na rzecz Odbudowy i Zwiększenia Odporności (672,5 miliarda euro). Państwa członkowskie Unii Europejskiej są zobowiązane do przeznaczenia minimum 20% środków na projekty cyfrowe³⁹.

Już w obecnie obowiązującym budżecie przewidziano 100 miliardów euro na program Horizon Europe, gdzie głównym celem było stworzenie międzynarodowych i międzyin-

39 https://pism.pl/publikacje/Wyzwania_zwiazane_z_wdrazaniem_instrumentu_na_rzecz_odbudowy_i_zwiekszenia_odpornosci

stytucjonalnych partnerstw. Międzynarodowe partnerstwa miały w dużej mierze dotyczyć finansowania badania i produkcji kluczowych technologii (np. półprzewodników). Międzyinstytucjonalne partnerstwa to głównie wsparcie rozwoju bezpiecznych sieci 5G i – w przyszłości – rozwoju nowej technologii 6G. Kolejne 10 miliardów euro ma zasilić Europejską Radę ds. Innowacji, która dysponowała budżetem rządu 3 miliardów euro na wsparcie start-upów. Jednym z wyzwań w przyszłym finansowaniu Horyzontu będzie bardziej równomierne dzielenie się środkami z tego programu. W poprzednim programie badawczym Horyzont 2020 95% środków przyznano tzw. starym członkom UE⁴⁰.

Pierwszy raz w historii w ramach Wieloletnich Ram Finansowych 2021-2027 stworzono osobny program dedykowany tylko transformacji cyfrowej – Cyfrowa Europa – z budżetem 9,2 miliarda euro. Miał on być kluczowy w przyciągnięciu 20 miliardów rocznych inwestycji na sztuczną inteligencję. W ramach tego programu planowane jest też przeznaczenie 2,2 miliarda euro na pracę nad budową europejskiego superkomputera. Program kwotą 850 milionów wesprze rozwój umiejętności cyfrowych obywateli. Ponadto 2 miliardy euro z Instrumentu Łącząc Europę zostaną przeznaczone na finansowanie infrastruktury 5G⁴¹.

Istnieją również inne pomysły zakładające zwiększenie inwestycji w technologię w UE. Autorzy raportu Eurostack wyszli z inicjatywą utworzenia funduszu o początkowej wartości 10 miliardów euro, który rósłby w czasie. Ich zdaniem powinien on wzrosnąć aż 30-krotnie w ciągu dekady. Środki miałyby pochodzić od państw członkowskich, Europejskiego Banku Inwestycyjnego, inwestorów instytucjonalnych oraz prywatnego kapitału. Sugeruje się również osobną ścieżkę budżetową na publiczną infrastrukturę cyfrową w ramach wieloletnich ram finansowania. Środki miałyby być przeznaczone na inwestowanie w sztuczną inteligencję, technologię chmurową oraz chipy, co miałyby się przyczynić do zmniejszenia zależności od nieeuropejskich BigTechów⁴².

Legislacja

Stworzenie od podstaw własnych, w pełni autonomicznych rozwiązań nie jest obecnie możliwe. Dlatego jednym z kluczowych podejść musi być współpraca z globalnymi dostawcami, którzy dostosowują swoje usługi do systemu prawnego stworzonego przez UE. W tym celu Unia Europejska zamierza wymusić przestrzeganie reguł wspólnoty poprzez szereg aktów prawnych. Wspólnota ma zamierzać powtórzyć sukces Rozporządzenia o Ochronie Danych Osobowych (RODO), które pomimo początkowych zastrzeżeń, okazało się dużym sukcesem. Weszło ono w życie w 2018 roku ujednolicając oraz wzmacniając przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osób⁴³. Wszystkie wielkie firmy z branży cyfrowej dostosowały się do nowych przepisów, a inne państwa na całym świecie przy wprowadzaniu regulacji o ochronie danych wzorowały się na RODO. Był to przykład

40 https://pism.pl/publikacje/Cyfrowa_dekada_UE_cele_i_wyzwania

41 https://pism.pl/publikacje/Cyfrowa_dekada_UE_cele_i_wyzwania

42 <https://www.techpolicy.press/the-quest-for-european-technological-sovereignty-building-the-eurostack/>

43 <https://uodo.gov.pl/404>

tego, jak można wzmocnić kontrolę nad danymi Europejczyków bez negatywnych skutków dla konkurencyjności⁴⁴. Jest to również ilustracja tzw. efektu brukselskiego, czyli sytuacji, w której przepisy UE wpływają na regulacje w innych krajach i na rynkach globalnych. W związku z tym Unia planuje podobne działania w obszarach uznawanych za kluczowe dla budowy cyfrowej suwerenności.

Jednym z najważniejszych wyzwań dla budowy cyfrowej suwerenności jest chmura obliczeniowa. W październiku 2025 roku Komisja Europejska zamówiła usługi chmurowe za 180 milionów euro na suwerenną chmurę, której celem jest wsparcie rynku i jego rozwój. Opublikowany dokument wprowadza wzór na obliczenie „wskaźnika suwerenności”. Jest on oparty na szeregu kategorii. Po pierwsze dana firma może zostać zakwalifikowana w ramach kategorii SEAL od 0 do 4, gdzie 4 oznacza pełną suwerenność cyfrową pozostającą całkowicie pod kontrolą Unii Europejskiej. Następnie oceniana jest w ramach 8 strategicznych celów:

- ▶ Strategiczna suwerenność
- ▶ Suwerenność prawna
- ▶ Suwerenność danych i sztucznej inteligencji
- ▶ Suwerenność operacyjna
- ▶ Suwerenność łańcucha dostaw
- ▶ Suwerenność technologiczna
- ▶ Bezpieczeństwo i zgodność
- ▶ Środowisko i zrównoważony rozwój

Otrzymany wynik jest podstawiany do wzoru na suwerenność cyfrową⁴⁵.

Wiosną 2026 ma wejść w życie ustawa o rozwoju chmury i sztucznej inteligencji (CAIDA). Jej celem jest zwiększenie pojemności unijnych centrów danych w ciągu najbliższych 5-7 lat i pełne zaspokojenie potrzeb przedsiębiorstw i administracji publicznej UE. Akt wzmocnienia cyfrowej suwerenności ma współgrać z proponowaną jednolitą, ogólnoeuropejską polityką dotyczącą usług chmurowych w administracji publicznej oraz w zamówieniach publicznych. Takie podejście ma sprzyjać rozwojowi europejskich dostawców usług w chmurze i priorytetowo traktować wykorzystanie wysoce bezpiecznej przepustowości chmury w kryzysowych sytuacjach⁴⁶. Rzecznik KE nie wyjaśnił, czy wskaźnik suwerenności będzie wpływał na formalną definicję suwerennych chmur w CAIDA⁴⁷.

Dobrym rozwiązaniem w ramach realizacji cyfrowej suwerenności jest wdrażanie koncepcji tzw. „cyfrowej ambasady”, polegającej na przenoszeniu kluczowych systemów państwowych za granicę w celu zabezpieczenia ich na wypadek scenariuszy kryzysowych. Taka sytuacja miała miejsce na Ukrainie, gdzie po rosyjskiej inwazji rząd przeniósł cały system

44 <https://countly.com/blog/importance-of-gdpr#:~:text=Meanwhile%2C%20from%20a%20governmental%20point,Vermont%2C%20to%20name%20a%20few.>

45 https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

46 <https://digital-strategy.ec.europa.eu/pl/policies/cloud-computing>

47 <https://tmt.expert/komisja-europejska-zamawia-uslugi-chmurowe-za-180-mln-eur-i-ustanawia-ramy-suwerennosci-chmury-2402/#:~:text=26%20pa%C5%BAdziernika%2C%202025-,Komisja%20Europejska%20zamawia%20us%C5%82ugi%20chmurowe%20za%20180%20mln%20EUR%20i,UE%E2%80%99>

administracji i finansów do chmury publicznej. Państwa UE, ale również sama Unia Europejska powinna opracować scenariusze awaryjne z wykorzystaniem własnej infrastruktury chmurowej⁴⁸. Warto podkreślić, że w UE już realizowane są konkretne projekty ukierunkowane na uzyskanie suwerenności cyfrowej w ramach chmury.

Jedną z flagowych inicjatyw jest projekt Gaia-X Europejskiego Stowarzyszenia na rzecz Danych i Chmury (AISBL) powołanego z końcem stycznia 2021. Jest to organizacja non-profit oferująca ekosystem rozwiązań i usług chmurowych. Pracuje nad stworzeniem środowiska, w którym dane mogą być udostępniane i przechowywane pod kontrolą ich właścicieli oraz użytkowników, zgodnie z jasno określonymi zasadami. Dane mają być łatwo dostępne, kompilowalne i wymienialne. W ramach Gaia-X współpracują dostawcy usług chmurowych, przedstawiciele świata nauki oraz różnorodni interesariusze, a celem organizacji jest opracowanie standardów funkcjonowania usług opartych na chmurze⁴⁹. Jest to ważny element tworzenia suwerennej infrastruktury chmurowej i przestrzeni danych. Gaia-X jest przykładem jak można finansować i budować europejską infrastrukturę umożliwiającą efektywne funkcjonowanie danych. Biorąc pod uwagę fakt, że cyfrowa suwerenność i strategiczna autonomia nie są obecnie jedną z opcji, lecz koniecznością, inicjatywa Gaia-X może odegrać kluczową rolę w zachowaniu pełnej kontroli nad europejską infrastrukturą cyfrową. Może stanowić narzędzie do efektywnego wykorzystania danych w badaniach, innowacjach i kształtowaniu polityki, a także zapewnić odpowiednią moc przetwarzania w obszarze sztucznej inteligencji. Ponadto Gaia-X ma potencjał odegrania istotnej roli w budowie Data Spaces — ekosystemów umożliwiających sprawną wymianę danych pomiędzy organizacjami, instytucjami publicznymi i prywatnymi firmami, zgodnie z określonymi ramami regulacyjnymi⁵⁰. Projekt Gaia-X spotkał się jednak z głosami krytyki. Była CEO francuskiego usługodawcy technologii chmurowych Scaleway i jedna z inicjatorek projektu nazwała go ogromną porażką, kolosalną stratą czasu i daniem kilku lat amerykańskim konkurentom. Rzeczywiście, od początku istnienia inicjatywy nie dokonano żadnych wdrożeń, a sama inicjatywa ugrzęzła w biurokratyczno-legislacyjnym impasie oraz politycznych bataliach⁵¹. Nowy CEO Gaia-X zapowiedział jednak konkretne działania wynikające ze sprzyjającego środowiska i wzrostu zainteresowania suwerennością cyfrową⁵².

W ramach działań mających na celu nadrobienie zaległości w produkcji półprzewodników Komisja Europejska zaproponowała European Chips Act (Akt w sprawie czipów). Jego głównym celem jest zapewnienie odporności łańcuchów dostaw oraz zmniejszenie zależności od zewnętrznych podmiotów. KE przedstawia ten akt jako kluczowy krok w kierunku suwerenności technologicznej i realizacji celu cyfrowej dekady, którym jest podwojenie udziału UE w światowym rynku półprzewodników do 20%.

48 <https://www.nask.pl/aktualnosci/suwerennosc-cyfrowa-pod-lupa-nask-na-kongresie-w-sejmie>

49 <https://piit.org.pl/partnerzy/gaia-x>

50 <https://www.computerworld.pl/article/3855389/gaia-x-wzmacnia-europejska-suwerennosc-cyfrowa.html>

51 <https://www.politico.eu/article/anatomy-franco-german-tech-misfire-american-dependence/>

52 <https://ing.dk/artikel/europes-response-cloud-giants-was-killed-within-ceo-now-promises-concrete-results>

Akt koncentruje się na pięciu strategicznych celach:

- ▶ wzmocnieniu badań naukowych;
- ▶ budowaniu i wzmacnianiu zdolności Europy do innowacji w zakresie projektowania, produkcji i pakowania zaawansowanych czipów;
- ▶ wprowadzeniu odpowiednich ram w celu zwiększenia produkcji do 2030 roku;
- ▶ rozwiązaniu problemu niedoboru wykwalifikowanej siły roboczej i przyciąganiu nowych talentów;
- ▶ rozwijaniu dogłębnego zrozumienia globalnego łańcucha dostaw półprzewodników⁵³.

Pięć celów European Chips Act opiera się na trzech filarach działania.

Pierwszy filar – „Czipy dla Europy” obejmuje wsparcie pięciu linii pilotażowych służących opracowywaniu, testowaniu i eksperymentowaniu z procesami oraz produkcji półprzewodników na małą skalę. Wszystkie państwa członkowskie utworzyły już centra kompetencji, które mają zapewnić przedsiębiorstwom niezbędne zasoby do opracowywania rozwiązań półprzewodnikowych.

Drugi filar koncentruje się na bezpieczeństwie dostaw i zwiększeniu odporności unijnego sektora półprzewodników. Działania te mają przyciągać inwestycje i zwiększać zdolności produkcyjne w UE. Komisja Europejska zatwierdziła siedem decyzji dotyczących pomocy państwa dla zakładów produkujących półprzewodniki.

Trzeci filar dotyczy monitorowania i reagowania kryzysowego. W jego ramach powołana została Europejska Rada ds. Półprzewodników, która pełni funkcję mechanizmu koordynacji między państwami członkowskimi a KE, umożliwiając monitorowanie unijnego łańcucha produkcji półprzewodników i zapobieganie potencjalnym kryzysom⁵⁴.

Jedną z najważniejszych technologii wymienianych w dokumentach strategicznych Unii Europejskiej jest akt o sztucznej inteligencji – pierwsza w skali świata kompleksowa regulacja prawna dla systemów i modeli sztucznej inteligencji. Celem rozporządzenia jest zapewnienie bezpieczeństwa, przejrzystości i zgodności z wartościami europejskimi w rozwoju i stosowaniu w całej UE. Uzależnia ona obowiązki dostawców i podmiotów wdrażających modele i systemy AI od potencjalnego ryzyka wyrządzenia szkód obywatelom, społeczeństwom i gospodarkom. Przepisy wprowadzają kategorię zakazanych praktyk w zakresie sztucznej inteligencji takich jak np. stosowanie rozwiązań opartych na technikach podprogowych, dyskryminujących określone grupy osoby czy stosowanie systemów AI do oceny obywateli. Akt zakłada również zwiększenie przejrzystości zastosowań systemów sztucznej inteligencji wysokiego ryzyka oraz nałożenie obowiązku gwarantowania przejrzystości poprzez sporządzenie dokumentacji technicznej⁵⁵. Nowa legislacja dotyczy głównie obszarów wysokiego ryzyka i kwestii bezpieczeństwa i ochrony danych, co wydaje się być fundamentem i jednym z filarów suwerenności cyfrowej UE.

53 <https://digital-strategy.ec.europa.eu/pl/policies/european-chips-act>

54 <https://digital-strategy.ec.europa.eu/pl/policies/european-chips-act>

55 <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Poza wspomnianymi wyżej aktami prawnymi istotne w koncepcji europejskiej cyfrowej suwerenności są Akt o Usługach Cyfrowych (DSA) i Akt o rynkach cyfrowych (DMA). Celem DSA jest stworzenie bezpieczniejszego środowiska internetowego dla konsumentów i przedsiębiorstw w UE poprzez określenie jasnych obowiązków dla platform internetowych i mediów społecznościowych, zwalczanie nielegalnych treści i produktów oraz osiągnięcie większej przejrzystości. Rozporządzenie wyznacza szereg przepisów, które muszą spełnić bardzo duże platformy internetowe (VLOP) oraz bardzo duże wyszukiwarki internetowe (VLOSE), które przede wszystkim powinny wykazywać większą transparentność w działaniu, jak również wykazać większą inicjatywę w zwalczaniu nielegalnych treści⁵⁶. Akt ma umożliwiać UE większą kontrolę nad infosferą UE i cyrkulacją danych.

DMA ma zagwarantować konkurencyjny i sprawiedliwy sektor cyfrowy, umożliwiający rozwój innowacyjnych przedsiębiorstw cyfrowych oraz zapewnienie bezpieczeństwa sieci poprzez m.in. jasne obowiązki i zakazy dla dużych platform internetowych, promowanie innowacji i bardziej sprawiedliwego środowiska platform internetowych dla nowych firm technologicznych czy zakazanie nieuczciwych praktyk stosowanych przez duże platformy internetowe. Główną zmianą, którą przynosi DMA to określenie dużych platform internetowych mianem „strażników dostępu” i wprowadzenie względem nich szeregu obowiązków. Strażnicy nie mogą m.in. śledzić użytkowników końcowych poza główną usługą platformy czy traktować własnych usług i produktów korzystniej niż analogiczne produkty podmiotów zewnętrznych. Celem regulacji jest przeciwdziałanie powstawaniu monopolu na rynku. Digital Markets Act (DMA) to akt, który podlega ewolucji; obecnie Komisja Europejska wszczęła badania rynku usług chmurowych w oparciu o DMA, mające ocenić, czy Amazon i Microsoft powinny zostać wyznaczeni jako „strażnicy dostępu” (gatekeepers) w zakresie usług w chmurze⁵⁷.

Współpraca międzynarodowa kluczem do budowy suwerenności cyfrowej

Unia Europejska budując pragmatyczną suwerenność cyfrową powinna współpracować z innymi globalnymi mocarstwami. Jedną ze ścieżek jest z całą pewnością utrzymanie współpracy ze Stanami Zjednoczonymi w ramach Rady ds. Handlu i Technologii⁵⁸. Innymi rozwiązaniami może być też szukanie bezpośredniej współpracy z poszczególnymi stanami USA, tak aby zwiększyć odporność na niestabilność ze strony rządu federalnego. Innym przykładem międzynarodowej współpracy mogłyby być spółki joint-venture z dynamicznie rozwijającym się kapitałem technologicznym z Indii, co pozwoliłoby na budowę wspólnych zdolności. Ramy handlowe z szybko rozwijającymi się azjatyckimi krajami ASEAN

56 <https://eur-lex.europa.eu/PL/legal-content/summary/digital-services-act.html>

57 <https://digital-strategy.ec.europa.eu/pl/news/commission-launches-market-investigations-cloud-computing-services-under-digital-markets-act>

58 Rada ta powstała w 2021 za kadencji prezydenta Bidena i była głównym forum współpracy w obszarze nowych technologii pomiędzy Stanami Zjednoczonymi i Unią Europejską. Powrót do władzy Donalda Trumpa i jego sceptyczne nastawienie do UE postawiło pod znakiem zapytania kontynuowanie współpracy w ramach tej inicjatywy. <https://www.pism.pl/publikacje/przyszlosc-rady-ds-handlu-i-technologii-za-prezydentury-donald-trump>

pozycjonują UE jako kraj wyznaczający standardy w zakresie cyfryzacji gospodarek dla tych państw, które poszukują alternatyw dla chińskiej infrastruktury lub amerykańskiej dominacji platformowej. Tworzenie tzw. odporności poprzez dywersyfikację, wydaje się być dobrym rozwiązaniem⁵⁹.

UE może także wykorzystać swoje przewagi strategiczne: w momencie, gdy poszczególne stany USA pracują nad odpowiednimi regulacjami, Bruksela ma możliwość wywierania znaczącego wpływu. Indie poszukujące partnerów do rozwoju przemysłu półprzewodników też mogą wykorzystać doświadczenia UE, podobnie jak państwa Azji Południowo-Wschodniej, które zamierzają cyfryzować swoją gospodarkę. UE może być tutaj architektem tworzenia programów naukowych, jak i wzorem budowania wspólnych standardów.

Świadome społeczeństwo i wykwalifikowani eksperci

Unia Europejska przywiązuje dużą wagę do edukacji, która pojawia się w kluczowych dokumentach strategicznych i politycznych dotyczących cyfryzacji. Budowa cyfrowej suwerenności nie jest możliwa bez społeczeństwa świadomego i sprawnego cyfrowo, potrafiącego w pełni wykorzystywać osiągnięcia technologiczne. Edukacja obejmuje także kształcenie wysoko wykwalifikowanych specjalistów w obszarze nowoczesnych technologii, z którymi Europa musi konkurować z Doliną Krzemową. Realizacja tych celów będzie kosztowna - niektóre szacunki wskazują na potrzebę pozyskania dodatkowych 500 tys. specjalistów, co może wiązać się z wydatkami rzędu 250 miliardów euro rocznie⁶⁰. UE może przyciągać specjalistów również poprzez dodatkowe atuty, takie jak lepsze warunki życia i pracy, płatny urlop, dostęp do opieki zdrowotnej oraz inne benefity socjalne.

Jedną z przeszkód na drodze do cyfrowej suwerenności UE jest fakt, że składa się ona z 27 państw o różnym stopniu cyfryzacji. Są państwa takie jak Estonia czy Finlandia, które znajdują się na czele, ale mamy też Bułgarię, które jest w ogonie stawki. To z pewnością utrudnia budowanie cyfrowej suwerenności.

Koncepcja europejskiego stosu technologicznego

Kolejnym pomysłem UE na zwiększenie cyfrowej suwerenności jest koncepcja europejskiego stosu technologicznego, tzw. EuroStack. Zaproponowana w 2024 roku, zakłada inwestycje w wysokości 300 miliardów euro na przestrzeni 10 lat w celu budowy europejskiej niezależności technologicznej, argumentując, że Europa stopniowo staje się cyfrową kolonią. Zainicjowana w środowiskach akademickich, koncepcja skupia obecnie ponad 260 sygnatariuszy, w tym największe firmy prywatne, takie jak Airbus. Jej głównym celem jest budowa publicznej cyfrowej infrastruktury o szerokim spektrum zastosowań.

59 <https://cepa.org/article/digital-sovereignty-can-europe-afford-it/>

60 <https://cepa.org/article/digital-sovereignty-can-europe-afford-it/>

EuroStack proponuje budowę cyfrowej suwerenności w oparciu o połączone warstwy zaawansowanych technologii, takich jak sztuczna inteligencja, półprzewodniki, technologie chmurowe oraz systemy kwantowe. Podejście przyjęte w ramach EuroStack promuje zrównoważony rozwój i interoperacyjność, odrzucając koncepcję pełnej samowystarczalności. Zamiast tego koncentruje się na budowie strategicznych zdolności, jednocześnie rozwijając międzynarodową współpracę przynoszącą korzyści wielu podmiotom. EuroStack nie stanowi sformalizowanych ram politycznych, lecz jest wezwaniem do działania, którego celem jest stworzenie autonomii strategicznej i integracja kluczowych technologii, takich jak sztuczna inteligencja, komputery kwantowe czy usługi chmurowe. Dzięki temu Unia Europejska zyskuje możliwość skutecznej rywalizacji na arenie globalnej⁶¹. EuroStack mógłby być finansowany z trzech źródeł: zamówień publicznych priorytetujących europejskie spółki, mobilizacji środków z unijnego rynku kapitałowego oraz funduszy w ramach unijnego budżetu na lata 2028-2034⁶².

Inny pomysłem jest wprowadzenie zmiany w dyrektywie o zamówieniach publicznych w celu wprowadzenia zmian wspierających lokalne przedsiębiorstwa z branży technologicznej. Klauzula nazywana Buy European zobowiązywałaby podmioty publiczne do nadania priorytetu dostawcom, którzy spełniają następujące kryteria takie jak:

- ▶ główna siedziba w Europie,
- ▶ większość działalności badawczo-rozwojowej w Europie,
- ▶ większościowa kontrola nad firmą sprawowana przez europejskie podmioty⁶³.

Rola państw członkowskich w budowie suwerenności cyfrowej UE

Jak już wspomniano, dużą słabością w budowaniu cyfrowej suwerenności UE może być fakt, że Unia składa się z 27 państw o zróżnicowanym poziomie rozwoju cyfrowego oraz różnej priorytetyzacji polityki cyfrowej i działań na rzecz suwerenności cyfrowej. Zamiast centralnego przyspieszenia, często dominuje rozproszenie kompetencji i brak koordynacji między państwami członkowskimi, a niekiedy nawet w obrębie poszczególnych krajów⁶⁴. Ponadto żadne pojedyncze państwo w Europie nie jest w stanie samodzielnie osiągnąć pełnej cyfrowej suwerenności.

Nie znaczy to jednak, że państwa członkowskie nie mogą być wartością dodaną dla budowy suwerenności cyfrowej. Często to właśnie w ich ramach funkcjonują rozwiązania, które można odwzorować w przypadku innych członków UE lub na poziomie samej UE. W Polsce dobrym przykładem jest projekt Krajowego Centrum Przetwarzania Danych (KCPD), aplikacja mObywatel czy system płatności BLIK. Francja używa własnego komunikatora

61 https://assets.filedock.xyz/public/EuroStack_2025.pdf, s. 6-9.

62 https://www.politykainsight.pl/_resource/multimedia/20393469, s. 5

63 https://www.politykainsight.pl/_resource/multimedia/20393469, s. 31

64 <https://www.forbes.pl/opinie/czy-polska-i-europa-zdaza-zbudowac-wlasna-suwerennosc-technologiczna/6mdgdr>

szyfrowanego w administracji publicznej, Estonia jest świetnym przykładem rozwoju usług elektronicznych, a Finlandia może być wzorem do rozwoju programów edukacyjnych. Dlatego też pojedyncze państwa mogą wnieść na poziom unijny własne, autorskie, sprawdzone rozwiązania. Należy też wziąć pod uwagę fakt, że nie zawsze własne rozwiązania odnoszą sukces. Francuska przeglądarka Qwant, stawiająca na ochronę prywatności użytkowników, okazała się nieudanym przedsięwzięciem.

Unia Europejska musi wypracować mądry i pragmatyczny sposób osiągnięcia cyfrowej suwerenności. Państwa członkowskie muszą pogodzić się z faktem, że tylko w ramach UE mogą w praktyce budować taką suwerenność, jednocześnie rezygnując z nierealistycznych postulatów nacjonalizacji usług cyfrowych. Doświadczenia poszczególnych krajów z różnymi projektami i inicjatywami technologicznymi, testowanymi na poziomie lokalnym, mogą jednak stanowić cenny element w procesie kształtowania europejskiej suwerenności cyfrowej.

Ciekawą hipotezę postawił Antonio Calcara w swoim artykule naukowym, twierdząc, że budowa suwerenności cyfrowej, której elementem ma być rezygnacja lub ograniczenie korzystania z rozwiązań firm nieeuropejskich może być elementem promowania własnych technologii przez państwa europejskie i wzmacniania ich pozycji. Jego zdaniem porażki w ramach budowy suwerenności cyfrowej nie doprowadzą do pogłębienia integracji, a postęp na poziomie UE jest instrumentalizowany dla korzyści krajowych. Ponadnarodowe ramy często łagodzą przepisy, aby dostosować się do działań krajowych w obliczu sceptycyzmu wobec scentralizowanych wydatków. W tym przypadku „postęp” ułatwia integrację negatywną (usuwanie barier wewnętrznych) i pozytywne działania (alokację zasobów), które uzupełniają strategie krajowe. Mechanizm ten obejmuje współpracę międzyrządową w celu przeciwdziałania konkurencji technologicznej z zagranicy, ale podziały wewnętrzne prowadzą do luźnej koordynacji, która umożliwia państwom dążenie do osiągnięcia korzyści dwustronnych. Zmienną zależną nie jest suwerenność całej UE, ale wzmocnienie ekosystemów krajowych, mierzone poprawą pozycji negocjacyjnej i partnerstw⁶⁵. Pomimo iż jego głos w dyskusji nie jest podzielany przez większość ekspertów, trzeba wskazać, że większość ewentualnych europejskich championów zlokalizowana byłaby w państwach starej Unii, głównie Niemczech i Francji. Może to prowadzić do sytuacji, że firmy z nowych państw członkowskich nie dostaną żadnego wsparcia i będą skazane na gorsze europejskie odpowiedniki.

65 <https://www.tandfonline.com/doi/full/10.1080/01402382.2025.2491962#abstract>

4. Trudna droga budowania suwerenności cyfrowej w obszarze 5G

Dotychczasowe doświadczenia z tworzenia suwerenności cyfrowej nie były niestety udane. Najlepszym przykładem jest tutaj kwestia sieci 5G, która została przez UE potraktowana strategicznie i uznana za priorytetową w budowaniu suwerenności cyfrowej. Pomimo posiadania dwóch dużych producentów sprzętu do budowy sieci 5G: szwedzkiego Ericssona i fińskiej Nokii oraz braku konkurencji ze strony Stanów Zjednoczonych, do dzisiaj nie udało się pokryć siecią 5G terenów UE zgodnie z założeniami. Dużym problemem było uzależnienie od jednego dostawcy (vendor lock-in) Huawei wśród operatorów telekomunikacyjnych i związana z tym konieczność kosztowanej wymiany infrastruktury, co do dzisiaj nie wszędzie się udało. W 2020 roku wprowadzono toolbox 5G, który miał umożliwiać wykluczanie dostawców wysokiego ryzyka (głównie z Chin), ich udział w rynku zmniejszył się tylko o 5-10%⁶⁶. Nie udało się również sprostać ambitnym terminom wdrożenia sieci 5G, a na przeszkodzie stanęły między innymi koszty⁶⁷.

Wydawać by się mogło, że technologia 5G może być perłą w europejskiej koronie technologicznej i załącznikiem tworzenia europejskiej suwerenności cyfrowej. Niestety pomimo posiadania dwóch z trzech największych producentów 5G i wsparcia Komisji Europejskiej, nie udało się zrealizować celów wdrażania rozwiązań technologicznych. Powinna to być cenna lekcja na przyszłość przy tworzeniu suwerenności cyfrowej, w szczególności, że w innych obszarach zidentyfikowanych jako kluczowe, UE nie ma takiego potencjału.

Suwerenność cyfrowa a firmy i użytkownicy

Budowanie suwerenności przez Unię Europejską to zarówno wyzwanie jak i wiele potencjalnych korzyści dla firm i użytkowników. Firmy i użytkownicy będą mniej podatni na zakłócenia w łańcuchach dostaw, ich cyberbezpieczeństwo i ochrona danych wzrosnie. Dla dużej liczby przedsiębiorstw będzie to również szansa na pozyskanie dodatkowych

66 <https://www.robert-schuman.eu/en/european-issues/817-the-european-strategic-approach-to-technological-security-the-challenges-posed-by-china>

67 <https://capacityglobal.com/news/europe-facing-5g-deployment-challenges/#:~:text=5G-,Europe%20facing%205G%20deployment%20challenges%20as%202025%20deadline%20approaches,schools%2C%20universities%2C%20and%20hospitals.>

funduszy i zaistnienie na rynku. Biznes dzięki licznym programom takim jak „Cyfrowa Europa” uzyska możliwość wsparcia dla transformacji cyfrowej. To jednak również wyzwania związane często z koniecznością wymiany sprzętu przykładowo wśród operatorów telekomunikacyjnych, znalezieniem nowych europejskich rozwiązań chmurowych – tutaj warto obserwować Airbusa czy też znalezienie alternatyw dla nieeuropejskich rozwiązań technologicznych. Może się to wiązać z dodatkowymi kosztami oraz koniecznością przeszkolenia personelu. Z pewnością to, czy firmy staną się beneficjentami budowy suwerenności cyfrowej będzie w dużej mierze zależało od ich otwartości na nowoczesne technologie i innowacje.

Suwerenność cyfrowa dla obywatela. Praktyczny poradnik:

- ▶ Dokonaj oceny pomiędzy bezpieczeństwem i prywatnością a potencjalnymi kosztami nowego rozwiązania;
- ▶ Śledź zmiany regulacyjne i zaadaptuj się do nich;
- ▶ Inwestuj w lokalne zasoby, takie jak centra danych, aby spełniać regulacje prawne;
- ▶ Strategicznie planuj zarządzanie danymi i sztuczną inteligencją uwzględniając wymogi przejrzystości i oceny ryzyka;
- ▶ Decydując o używanych narzędziach wybieraj interoperacyjne rozwiązania;
- ▶ Nie uzależniaj się od jednego dostawcy, dywersyfikuj ich. Podejmuj decyzje, które pozwalają na swobodną migrację danych i elastyczne łączenie różnych rozwiązań;
- ▶ Oceniaj ryzyko geopolityczne i cyberbezpieczeństwa.

Negatywne skutki tworzenia się suwerenności cyfrowej

Proces kształtowania się suwerenności cyfrowej może przynieść wiele dobrego Unii Europejskiej, pomagając jej w zwiększaniu konkurencyjności. Niestety nieroztropne kroki, zbyt duże przywiązanie do legislacji, a czasami wręcz przeregulowanie niektórych sektorów, może mieć negatywne konsekwencje, takie jak opóźnienie dostępu do najnowszych technologii, dławienie innowacyjności, utrudnianie działania małych i średnich firm czy też wpływanie na komfort pojedynczego użytkownika.

Najlepszym przykładem jest rozwój autonomicznych samochodów w Unii Europejskiej, który pozostaje w tyle za Chinami czy Stanami Zjednoczonymi. Jednym z powodów takiej sytuacji jest wymóg szeroko zakrojonych testów i certyfikacji systemów autonomicznych, które często różnią się od siebie w różnych państwach. Część członków UE wymaga dodatkowych testów, a legislacja często się zmienia i trudno się do niej dostosować. To negatywnie wpływa na rozwój samochodów autonomicznych. Podobnie jak rygorystyczne przepisy odnoszące się do ochrony danych osobowych. Wprowadzie istnieją pilotaże wdrażania tej technologii, ale przejście do pełnej autonomii jest utrudniane w dużej mierze przez brak harmonizacji prawa. Oczywiście nie można zapomnieć, że europejskie miasta wyglądają inaczej niż ich amerykańskie i chińskie odpowiedniki i sama architektura utrudnia budowanie odpowiedniej infrastruktury koniecznej do wdrażania samochodów autonomicznych⁶⁸.

68 <https://www.nature.com/articles/s44333-025-00055-3>

Regulacje mogą też wpływać na dostępność niektórych technologii proponowanych przez BigTechy. Tak się stało z modelami AI od Mety, które nie zostały wprowadzone w UE, po tym jak irlandzki organ regulacyjny ds. prywatności nakazał opóźnienie wdrażania planu wykorzystania danych użytkowników Facebooka i Instagrama. Meta argumentowała, że będzie korzystać wyłącznie z publicznie dostępnych i licencjonowanych informacji online, nie zmieniło to jednak decyzji organu. Abstrahując od tego czy obawy o prywatność są uzasadnione, skutkiem unijnej legislacji był brak technologii na terenie UE⁶⁹. Pomimo tego, że legislacja unijna ma co do zasady uderzać w BigTechy, dając szansę małym i średnim przedsiębiorstwom (MŚP), okazuje się, że czasem może ona szkodzić również im. Taka możliwość występuje w ramach Digital Fairness Act (DFA), który ma zapewniać konsumentom ochronę przed nieuczciwymi i manipulacyjnymi praktykami w Internecie. Przedstawiciele MŚP obawiają się ograniczenia możliwości personalizacji reklamy i systemów rekomendacji, co przełoży się na ograniczoną zdolność firm do docierania do klientów i ich pozyskania. Część przedstawicieli MŚP obawia się spadku konkurencyjności małych firm i przejęcia rynku przez gigantów⁷⁰. Nie tylko DFA wzbudza obawy MŚP - podobnie sytuacja wygląda z DMA, który nakłada kosztowne obciążenia związane z przestrzeganiem przepisów, spowalniających rozwój startupów, których UE rozpaczliwie potrzebuje. Na problem nadmiernej, niejasnej i niezgodnej regulacji zatrzymującej rozwój innowacyjnych firm w Europie, wskazywał raport Draghiego. To regulacyjne zamieszanie zniechęca startupy do rozwoju i ekspansji transgranicznej, ponieważ obawiają się one ciągle zmieniających się przepisów i wynikających z nich nowych obowiązków, co ostatecznie uniemożliwia im osiągnięcie poziomu europejskich liderów. Ustawa DMA nakłada na MŚP pośrednie, ale nieuniknione obciążenia związane z przestrzeganiem przepisów, co może prowadzić do wyczerpania ich ograniczonych zasobów i odwraca uwagę od innowacji.

Budowanie suwerenności cyfrowej może też negatywnie wpływać na pojedynczych użytkowników, jak ma to miejsce w przypadku Aktu o rynkach cyfrowych (DMA). Jednym z najbardziej znanych przykładów jest utrudnienie korzystania z Google Maps, ze względu na fakt, że zniknął bezpośredni link do Map Google z górnego paska wyniku wyszukiwania, co utrudnia korzystanie z usługi. Inną problematyczną kwestią jest klikanie w formularze dot. cookies na każdej stronie internetowej. Większość użytkowników klika w nie, nawet nie czytając, co utrwała najgorszy możliwy zwyczaj wśród internautów – klikania w treści bez ich przeczytania, co może stanowić zagrożenie dla ich bezpieczeństwa⁷¹.

69 <https://www.press.pl/tresc/82222,meta-wstrzymuje-wprowadzanie-swoich-modeli-ai-w-europie#:~:text=Meta%20Platform%20na%20razie%20nie%20b%C4%99dzie%20wprowadza%C4%87,planu%20wykorzystywania%20danych%20u%C5%B4Cytownik%C3%B3w%20Facebooka%20i%20Instagrama.>

70 <https://www.bankier.pl/wiadomosc/Nowe-unijne-przepisy-a-przyszlosc-MSP-Czy-Digital-Fairness-Act-ograniczy-rozwoj-polskich-firm-9030508.html>

71 <https://itif.org/publications/2025/06/30/six-ways-the-dma-is-backfiring-on-europe/>

Zakończenie

Koncepcja suwerenności cyfrowej powróciła do łask i znowu staje się często dyskutowanym tematem. Jest to jednoznacznie powiązane z sytuacją geostrategiczną, zmianą paradygmatu globalizacji, coraz bardziej asertywną postawą Chin, ale przede wszystkim nowym podejściem administracji Trumpa do stosunków transatlantyckich. Tym razem wydaje się, że koncepcja ta, nie będzie jedynie ograniczona do strategicznych i politycznych dokumentów, ale będzie faktycznie wprowadzana. Sygnałem zmiany są duże fundusze zadeklarowane przez UE, ale też postawa Airbusa – jednej z największych firm w UE, która zamierza częściowo zrezygnować z usług Google i Microsoft, stawiając na europejskiego dostawcę chmury, powołując się przy tym na kwestie związane z bezpieczeństwem.

Z dokumentów Unii Europejskiej wyłania się koncepcja suwerenności cyfrowej, która nie ma nic wspólnego z totalną samowystarczalnością, jak ogłaszają to państwa autorytarne, a raczej pragmatycznym i coraz bardziej praktycznym podejściem. Osiągnięcie pełnej autarkii przez UE byłoby praktycznie niemożliwe i niezwykle kosztowne, dlatego ten cel nie znajduje odzwierciedlenia w nawet najbardziej ambitnych dokumentach Wspólnoty. Unia Europejska ma zamiar budować swoją suwerenność cyfrową poprzez następujące główne elementy: finansowe wsparcie dla sektora cyfrowego płynące z różnych programów, które umożliwi budowę europejskich rozwiązań technologicznych oraz rozwiniętą legislację, dzięki której BigTechy będą musiały się dostosować do prawnego reżimu UE. Bruksela wie, że skoro udało się to zrobić z RODO, to podobnie sytuacja będzie wyglądała z innymi regulacjami. Pytanie, czy to założenie nie okaże się błędne, a zmniejszająca się rola UE na świecie, nie doprowadzi do spadku znaczenia i wpływu efektu brukselskiego⁷².

W obszarze autonomii, UE zamierza przede wszystkim sprawować kontrolę nad danymi Europejczyków oraz chronić krytyczne dane i usługi. Model, który zapowiedział Airbus, jeżeli okaże się sukcesem, może być punktem odniesienia dla innych europejskich firm, które podążą jego drogą. Jednak brak sukcesu na tym polu może być silnym ciosem uderzającym w budowanie europejskiej suwerenności cyfrowej. Warto też podkreślić, że decyzja Airbusa nie jest podyktowana konkretnym rozwiązaniem prawnym, a wychodzi z konieczności biznesowej. UE w ramach budowania suwerenności cyfrowej może też korzystać z doświadczeń poszczególnych państw - np. Francji, która rozwija swoje autonomiczne oprogramowanie, ale ma też ograniczenia, co pokazał falstart francuskiej przeglądarki internetowej Qwant.

Unia Europejska nie powinna koncentrować się na stworzeniu wiernej kopii Doliny Krzemowej czy innych rozwiązań technologicznych, ale raczej skupiać się na budowaniu przewag konkurencyjnych i znalezieniu odpowiedniego pomysłu biznesowego. Przykład Zalando, Spotify czy ElevenLabs pokazuje, że jest to jak najbardziej wykonalne w UE. To równie przy-

72 <https://www.ft.com/content/abc3002e-a7be-48e2-8197-aeddf937afec>

kład udanej współpracy transatlantyckiej, ponieważ ich sukces nie byłby możliwy bez wykorzystania infrastruktury chmurowej amerykańskich hyperscalerów oraz funduszy z USA czy prywatnych inwestorów.

Warto również wykorzystywać własne atuty i dążyć do tego, by europejskie miasta stały się miejscem, gdzie inżynierowie z Indii, amerykańscy naukowcy i przedsiębiorcy z Afryki chcą ze sobą współpracować. UE może być technologicznym tygłem kulturowym, gdzie krzyżują się perspektywy na technologie z całego świata⁷³.

Tworzenie suwerenności cyfrowej to ciągły proces, który nigdy się nie kończy. Celem pragmatycznego modelu suwerenności cyfrowej nie powinno być dążenie do eliminacji globalnych dostawców, ale zdolność do kontroli, audytu i zmiany, jeżeli będzie taka potrzeba. Wymaga on elastycznego modelu zarządzania, który szybko reaguje na zmiany zarówno technologiczne jak i rynkowe oraz adaptuje się do nich. Jest to niestety bardzo trudne biorąc pod uwagę funkcjonowanie UE jako biurokratycznego molocha. Suwerenność cyfrowa nie powinna być projektem tylko dla informatyków czy prawników, a raczej być traktowana jako pewien kontrakt pomiędzy państwem, biznesem i obywatelami. Żyjemy w czasach, kiedy dane są paliwem gospodarki, algorytmy decydują o dostępie do usług, a kontrola nad infrastrukturą cyfrową staje się formą sprawczości państwa⁷⁴. Duże poparcie dla tej koncepcji wśród społeczeństw europejskich daje nadzieję na pozytywne zmiany w tym obszarze⁷⁵.

Unia Europejska powinna potraktować osiągnięcie suwerenności technologicznej priorytetowo, podobnie jak podeszła do kwestii bezpieczeństwa energetycznego po rosyjskiej inwazji na Ukrainę. W tym celu trzeba wzmocnić kompetencje, rozbudować infrastrukturę cyfrową i jasno zdefiniować cele tak aby cyfrowa suwerenność przestała być tylko sloganem, a stała się filarem gospodarki polskiej i europejskiej⁷⁶. Tworząc własną suwerenność cyfrową, podobnie jak w przypadku suwerenności energetycznej, Unia Europejska zyska odporność na zakłócenia zewnętrzne i szantaż ze strony coraz bardziej asertywnych państw jak Chiny czy Stany Zjednoczone.

73 <https://cepa.org/article/digital-sovereignty-can-europe-afford-it/>

74 <https://www.forbes.pl/opinie/czy-polska-i-europa-zdaza-zbudowac-wlasna-suwerennosc-technologiczna/6mdgdrt>

75 <https://legrandcontinent.eu/fr/2025/09/25/souverainete-technologique--10-points/>

76 <https://www.forbes.pl/opinie/czy-polska-i-europa-zdaza-zbudowac-wlasna-suwerennosc-technologiczna/6mdgdrt>

NOTA REDAKCYJNA

Niniejszy raport został przygotowany jako materiał analityczny poświęcony zagadnieniu suwerenności technologicznej w Unii Europejskiej i państwach członkowskich, ze szczególnym uwzględnieniem wymiaru cyfrowego, cyberbezpieczeństwa, chmury obliczeniowej oraz sztucznej inteligencji.

Raport powstał w odpowiedzi na narastającą potrzebę uporządkowania debaty wokół suwerenności technologicznej, która coraz częściej prowadzona jest w sposób uproszczony, ideologiczny lub oderwany od realiów operacyjnych, ekonomicznych i bezpieczeństwa.

Celem publikacji jest wniesienie do tej debaty perspektywy pragmatycznej, opartej na analizie ryzyk, zdolności instytucjonalnych państw oraz realnych mechanizmów kontroli technologicznej - a nie na postulatach pełnej autarkii czy izolacji technologicznej.

CEL I ZAKRES RAPORTU

Celem raportu jest:

- ▶ zaproponowanie spójnego, operacyjnego modelu suwerenności technologicznej,
- ▶ identyfikacja kluczowych ryzyk i ograniczeń obecnych podejść regulacyjnych,
- ▶ wskazanie możliwych kierunków działań dla decydentów publicznych, regulatorów oraz instytucji odpowiedzialnych za cyberbezpieczeństwo.

Raport koncentruje się na:

- ▶ politykach i regulacjach UE,
- ▶ praktyce państw członkowskich,
- ▶ roli globalnych i europejskich dostawców technologii,
- ▶ konsekwencjach dla administracji publicznej, gospodarki i obywateli.

Raport nie jest:

- ▶ dokumentem lobbingowym,
- ▶ stanowiskiem rządu, instytucji unijnych ani partnerów komercyjnych,
- ▶ rekomendacją wyboru konkretnych dostawców technologicznych.

METODOLOGIA

Raport został opracowany w oparciu o:

- ▶ analizę obowiązujących i projektowanych regulacji UE (m.in. NIS2, DORA, inicjatywy cloudowe i AI),
- ▶ analizę publicznie dostępnych dokumentów strategicznych i eksperckich,
- ▶ przegląd studiów przypadków z państw UE i spoza UE,
- ▶ analizę porównawczą modeli zarządzania ryzykiem technologicznym,
- ▶ konsultacje eksperckie i dyskusje robocze.

Wnioski raportu mają charakter analityczny i syntetyczny. Ich celem nie jest rozstrzyganie sporów ideologicznych, lecz wskazanie możliwych, realistycznych scenariuszy działania.

DEFINICJA SUWERENNOŚCI TECHNOLOGICZNEJ (NA POTRZEBY RAPORTU)

Na potrzeby niniejszego raportu suwerenność technologiczna rozumiana jest jako:

Zdolność państwa i jego instytucji do podejmowania niezależnych decyzji technologicznych, kontroli kluczowych danych i procesów, audytu rozwiązań oraz zmiany dostawców - przy jednoczesnym świadomym korzystaniu z rozwiązań rynkowych, w tym globalnych, jeśli spełniają one określone kryteria bezpieczeństwa i kontroli.

Suwerenność technologiczna nie jest utożsamiana z:

- ▶ pełną samowystarczalnością technologiczną,
- ▶ eliminacją zagranicznych technologii,
- ▶ przymusowym stosowaniem rozwiązań narodowych lub regionalnych.

ROLA PARTNERÓW I INTERESARIUSZY

Raport został przygotowany na zlecenie Instytutu Poznańskiego.

Partnerzy wspierający proces powstawania raportu:

- ▶ uczestniczyli w dyskusjach eksperckich,
- ▶ dzielili się wiedzą i doświadczeniem branżowym,
- ▶ nie mieli wpływu na ostateczne brzmienie wniosków ani rekomendacji.

Partnerzy nie posiadają prawa weta wobec treści raportu ani jego konkluzji.

Odpowiedzialność za treść raportu ponoszą wyłącznie autorzy i wydawca.

ADRESACI RAPORTU

Raport kierowany jest w szczególności do:

- ▶ decydentów publicznych i administracji państwowej,
- ▶ regulatorów i instytucji odpowiedzialnych za cyberbezpieczeństwo,
- ▶ środowisk eksperckich i analitycznych,
- ▶ przedstawicieli sektora technologicznego,
- ▶ dziennikarzy zajmujących się tematyką cyfryzacji i bezpieczeństwa.

CHARAKTER REKOMENDACJI

Zawarte w raporcie rekomendacje:

- ▶ mają charakter strategiczny i operacyjny,
- ▶ nie są prawnie wiążące,
- ▶ stanowią materiał pomocniczy w procesach decyzyjnych.

Ostateczne decyzje dotyczące polityk publicznych, regulacji i wdrożeń technologicznych pozostają w gestii właściwych organów.

ZASTRZEŻENIE

Raport odzwierciedla stan wiedzy i analizy na moment jego przygotowania. Dynamiczny charakter technologii, regulacji oraz zagrożeń cybernetycznych może wpływać na aktualność niektórych wniosków w dłuższej perspektywie czasowej.

O suwerenności cyfrowej
podyskutujesz również

na

V edycji Poznańskiego Kongresu Gospodarczego!



**Poznański
Kongres
Gospodarczy**

Zapraszamy!
3-4 grudnia 2026 r.

Poznań Congress Centre
Międzynarodowe Targi Poznańskie

www.kongres.poznanski.org



Instytut Poznański

www.poznanski.org

instytut@poznanski.org



Suwerenność Cyfrowa

Między autonomią
a pragmatyzmem

dr Andrzej Kozłowski