SUWERENNOŚĆ TECHNOLOGICZNA POLSKI I EUROPY

Raport z badania opinii społecznej. Edycja 2026.

digitalpoland

Tytuł raportu: Suwerenność technologiczna Polski i Europy. Raport z badania opinii społecznej. Edycja 2026.

Edycja: 1 | Warszawa, marzec 2026 r.

ISBN: 978-83-971647-7-2

Wydawca: Fundacja digitalpoland

digitalpoland

Stępińska 22/30, 00-739, Warszawa, Polska
info@digitalpoland.org | digitalpoland.org | digitalfestival.pl | digitalshapers.pl | digitalars.pl | aipoland.org | eaiforum.org

Finansowanie: Publikacja sfinansowana ze środków pozyskanych od Partnerów raportu przeznaczonych na edukację społeczeństwa oraz statutowych.

Partnerzy raportu: APATOR, Billennium, home.pl, OKTAWAVE, PIKE Polska Izba Komunikacji Elektronicznej, SUSE, Polska Chmura

Redakcja: Piotr Mieczkowski

Podziękowania: Fundacja Digital Poland pragnie podziękować Partnerom raportu i Fundatorom, dzięki którym może realizować swoją misję. Więcej informacji na digitalpoland.org/kto

Projekt, DTP: Krzysztof Waloszczyk | So! Creative House | www.socreativehouse.pl

SPIS TREŚCI

4 PRZEDMOWA

6 JAK CZYTAĆ RAPORT

8 PODSUMOWANIE ZARZĄDCZE

14 WPROWADZENIE

20 BADANIE OPINII PUBLICZNEJ

43 PRZEGLĄD DZIAŁAŃ INNYCH PAŃSTW Z ZAKRESU SUWERENNOŚCI TECHNOLOGICZNEJ

77 O BADANIU OPINII PUBLICZNEJ

81 AUTORZY I EKSPERCI PUBLIKACJI

84 O FUNDACJI DIGITAL POLAND I DIGITAL FESTIVAL 2025

PRZEDMOWA

dr Michal Boni

Prezes Fundacji Digital Poland, Adiunkt na uniwersytecie SWPS, Członek Europejskiego Komitetu Ekonomiczno Społecznego

Od kilku lat temat suwerenności technologicznej, głównie cyfrowej staje się coraz bardziej gorąco dyskutowany. Świadomość uzależnienia od amerykańskich graczy nabiera znaczenia i rodzi pytania i wątpliwości (od 2017 roku 70% modeli AI powstało w USA, 70% przetwarzania w chmurze w Unii Europejskiej odbywa się za sprawą Microsoft'a, Amazon'a, Google'a, europejskie wydatki na badania dotyczące software i internetu, to 7% globalnych). Zwrot geopolityczny, jakiego dokonuje Prezydent Trump potęguje zagrożenia, nie mówiąc o bezpośrednich atakach np. Elona Muska na europejskie regulacje prawne, które mają chronić prywatność i obywateli przed nienawistnymi atakami innych. Debaty o NATO, o Grenlandii, o cłach, presja jaką administracja amerykańska wywiera na europejskie wartości - wszystko to tworzy kolizyjny tor dotychczasowo dobrej współpracy transatlantyckiej.

Dlatego suwerenność, która nigdy nie będzie i nie powinna być europejską autarkią w sprawach transformacji cyfrowej - jest tak istotna dla przyszłego rozwoju. I cieszy badanie, którego wyniki Państwo otrzymujecie w niniejszym Raporcie.

56% badanych opowiada się za suwerennością technologiczną. To więcej, niż połowa, ale czy to dużo ? Czy wystarczająco, by budować polityki na rzecz suwerenności ? Przy dyskusji w Polsce o programie SAFE (wielkie inwestycyjne wsparcie dla Polski na rzecz rozwoju obronności - niskooprocentowana pożyczka pieniędzy, do nas trafia 43,7 mld euro), de facto niepoważnych pytaniach Prezydenta RP i szerzeniu obaw, iż Polska uzależni się od europejskich producentów (Francja, Niemcy), i że tylko USA powinny być kontraktorem - rozkład poglądów w Sieci (badania Sieci – ResFutura.pl) wyglądał następująco: 32% wsparcie dla Programu, a 68% krytyka i zarzuty, że to zadłużanie państwa, że wszystko zostanie przekazane na Ukrainę. Kto miesza w głowach i bardzo praktycznie - osłabia akceptację działań na rzecz suwerenności technologicznej?

A przecież równolegle, i raport to pokazuje, 45% osób deklaruje zaufanie do krajowych rozwiązań cyfrowych czy technologicznych. Nie jest to dziwne, bo jeśli 11 mln obywateli korzysta z ePUAP, MojeIKP, mObywatela, mZUSu, to znaczy, iż zaufanie buduje się nie na hasłach, ale na konkretach. Wiarygodność następnych kroków w cyfryzacji usług administracyjnych, opartych o polskie rozwiązania, będzie miała kolosalne znaczenie dla budowania suwerenności technologicznej kraju.

Aczkolwiek dzisiaj tylko 24% uważa, iż jesteśmy przygotowani do stworzenia ram dla suwerenności cyfrowej (42% nie ma zdania, co oznacza, że mogą być otwarci na wyjaśnienia). Wątpliwości pojawiają się w odniesieniu do zagrożeń wobec infrastruktury krytycznej – czy mamy naprawdę zabezpieczenia na wypadek ataków, zdalnego jej wyłączania, wojny hybrydowej. Ale jako ryzyko traktowane bywają też nachalne praktyki dużych graczy i platform: przeciw prywatności, z wymuszeniem wyboru konsumenckiego, z nasycaniem treści prymitywizmem, nienawiścią i emocjami chwili - algorytmy traumy, czy trajektorie dezinformacji. Obawy budzi groźba szpiegostwa i inwigilacji wpisanej w urządzenia i systemy (chińskie, w części amerykańskie), a także odcięcia od produktów niezbędnych w rozwoju technologicznym, jak półprzewodniki. Respondenci wskazywali również na groźbę presji dokonywanej przez kraje trzecie - co robią Amerykanie chcąc wymóc odejście w Europie od praw regulujących transparentność AI, czy reguły odpowiedzialności platform za treści, jakie tam się pojawiają.

Ciekawym elementem badania było pytanie dotyczące, jak odpowiadać na zagrożenia. Niektóre z odpowiedzi okazały się chybione - jako remedium na wzrost dezinformacji wskazywano zastosowanie przepisów wobec treści łamiących prawo takich, jakie funkcjonują w odniesieniu do mediów. To jakby odpowiedź z dawnej epoki. Dziś tradycyjne media tak samo mogą sieją dezinformację, jak społecznościowe , a ponadto - narzędziem jest wdrożenie regulacji o usługach cyfrowych (DSA), co uniemożliwił w Polsce Prezydent RP. I dzieje się to pod hasłami obrony wolności w internecie, gdy tymczasem wolność bez odpowiedzialności nie jest wolnością, nawet jeśli Prezydent Trump i Elon Musk uważają (a za nimi polski Prezydent RP) inaczej.

Szczęśliwie badanie pokazało, że myślenie o tworzeniu suwerenności technologicznej nie może się udać poprzez wyłączność krajowych rozwiązań.

Dominuje przekonanie, że musi to być mix wysiłków - krajowych i europejskich, a kraje trzecie ze swoimi technologiami mogą i powinny być graczami na rynku, ale z pełnym respektem dla reguł i prawa europejskiego.

Przeczytajcie Raport!!! Bardzo ciekawy!!!

JAK CZYTAĆ RAPORT

Raport przedstawia wyniki reprezentatywnego badania polskiego społeczeństwa na suwerenności technologicznej

O raporcie

W fundacji regularnie podejmujemy się realizacji kompleksowych badań dotyczących kluczowych wyzwań cyfryzacji. W latach ubiegłych zbadaliśmy m.in. nastawienie Polaków do sztucznej inteligencji (AI), wiedzę na temat cyberbezpieczeństwa czy łączności.

W tym roku, z uwagi na bezprecedensowe wyzwania, przed którymi stoi nasza część świata, w tym m.in. :

a) **rosnące napięcia geopolityczne**, niestabilność globalnych łańcuchów dostaw oraz postępującą utratę zasobów wiedzy, miejsc pracy i zdolności przemysłowych w obszarze technologii krytycznych na poziomie naszego kraju i całej UE,
b) **rosnącą rolę infrastruktury krytycznej**, bez której państwo po prostu przestaje funkcjonować (co dobitnie pokazał niedawny blackout energetyczny w Hiszpanii), oraz ryzyko zdalnego wyłączania kluczowych usług przez podmioty zewnętrzne (jak w przypadku ograniczania działania systemu Starlink przez Elona Muska podczas wojny w Ukrainie),
c) **dominację pozaeuropejskich gigantów technologicznych**, utratę pełnej kontroli nad danymi oraz nasilające się szpiegostwo przemysłowe,
d) **rosnące ryzyko wykorzystywania technologii przez państwa trzecie jako narzędzia nacisku** (np. szerzenie dezinformacji, groźby zerwania stosunków dyplomatycznych) w celu wywierania presji na Polskę lub Unię Europejską w sytuacjach konfliktów handlowych lub geopolitycznych,
e) **rosnący wpływ pozaeuropejskich platform społecznościowych** (np. TikTok, X, Instagram, YouTube) na procesy demokratyczne, w tym rozprzestrzenianie dezinformacji i wpływanie na wyniki wyborów, co mogliśmy zaobserwować np. w Rumunii oraz trwającą w całej Unii Europejskiej dyskusję o konieczności budowy niezależności gospodarczej,

postanowiliśmy przeprowadzić pierwsze tak kompleksowe w Polsce **badanie opinii publicznej na temat suwerenności technologicznej**.

W naszych pracach zawsze kierujemy się analizą danych i formułowaniem rekomendacji na bazie twardych faktów. Niniejszym raportem pragniemy dostarczyć konkretny materiał do debaty publicznej oraz wesprzeć proces kształtowania polityk państwowych i unijnych. Przy tworzeniu kwestionariusza opieraliśmy się na najlepszych światowych praktykach, a same pytania konsultowaliśmy z wiodącymi ekspertami rynkowymi oraz przedstawicielami sektora pozarządowego.

Jak czytać raport?

Aby ułatwić szybkie zrozumienie danych, przy większości głównych pytań umieściliśmy ikony ilustrujące wyniki dla konkretnych grup badanych. Analiza została przeprowadzona w podziale na podstawowe segmenty demograficzne: płeć, pokolenie (wiek), miejsce zamieszkania oraz wykształcenie.

Ze względu na ograniczoną objętość publikacji i w trosce o jej maksymalną przejrzystość, na infografikach prezentujemy zazwyczaj jedynie skrajne podsegmenty – na przykład zestawiamy opinie mieszkańców wsi z odpowiedziami mieszkańców największych metropolii, albo poglądy osób z wykształceniem podstawowym z tymi po studiach wyższych. Grupy pośrednie (np. mieszkańcy średnich miast), których odpowiedzi najczęściej były zbliżone do średniego wyniku dla całej populacji, zostały pominięte w wizualnych zestawieniach, aby wyeksponować to, co najbardziej różnicuje polskie społeczeństwo.

PODSUMOWANIE ZARZĄDCZE

Anatomia utraty suwerenności

Obecne uzależnienie Europy od globalnych gigantów technologicznych nie jest dziełem przypadku, lecz efektem wieloletnich zaniechań i błędnych założeń strategicznych w Europie i Polsce. Do kluczowych czynników należą:

- **asymetria handlowa i produkcyjna** - otwartość granic UE zderzyła się z barierami rynkowymi w Azji. Dodatkowo, błędnie założono, że przeniesienie produkcji na Daleki Wschód nie przyniesie negatywnych skutków, co w rzeczywistości doprowadziło do utraty bezcennego know-how.
- **pułapka „darmowych" usług i drenaż danych** - oddanie najcenniejszych danych przedsiębiorców i konsumentów globalnym platformom stało się fundamentem do stworzenia przez nich potęgi w obszarze sztucznej inteligencji (AI) i nowych produktów.
- **brak europejskiego kapitału i ochrony** -brak jednolitego rynku kapitałowego sprawił, że oszczędności Europejczyków finansują (co jest kuriozalne!) amerykańskie platformy, wypierając własne rozwiązania na terenie UE. Równocześnie nieskuteczne prawo antymonopolowe sprawiło, że kary dla big techów stały się dla nich jedynie zwykłym kosztem prowadzenia biznesu wymuszając większe środki na lobbing i astroturfing.

Skutki braku niezależności

Brak suwerenności technologicznej uderza bezpośrednio w krajowe firmy i bezpieczeństwo państwa, generując szereg krytycznych ryzyk:

- **dławienie krajowego biznesu** - firmy w suwerennych krajach generują marże na poziomie 25-35%, podczas gdy w UE, jako biorców technologii, spadają one do 5-10%. Generuje to gigantyczny deficyt handlowy w usługach cyfrowych, szacowany w Polsce ok. 45 mld PLN. Dodatkowo, krajowe MŚP są dyskryminowane w przetargach pisanych pod dyktando globalnych marek.
- **zagrożenia dla bezpieczeństwa i ciągłości działania** - istnieje realne ryzyko paraliżu operacyjnego z powodu braku komponentów (np. półprzewodników) oraz tzw. „kill switch", czyli zdalnego odcięcia państwa od kluczowych usług. Wzrasta również zagrożenie szpiegostwem, utratą własności intelektualnej oraz manipulacją procesami demokratycznymi za pomocą zagranicznych platform i algorytmów AI.

Zwrot ku polityce przemysłowej i mądremu interwencjonizmowi

Od 2019 roku obserwujemy na świecie bezprecedensowy renesans polityki przemysłowej i gwałtowny wzrost interwencji państwowych. W obliczu agresywnego dotowania własnych firm przez inne mocarstwa, bierność Polski grozi marginalizacją. Skuteczny interwencjonizm nie polega na ślepym protekcjonizmie, lecz na precyzyjnym wspieraniu B+R z użyciem tzw. klauzul wygasania (*sunset clauses*), aby nie uzależniać firm od państwowych dotacji.

Paradygmat Innowacji - produkcja warunkuje B+R

Raport obala mit, że same inwestycje w startupy wystarczą do zbudowania przewagi. Znaczące innowacje są pochodną posiadania własnej produkcji i nie rodzą się w izolacji od niej. Aby B+R budowało suwerenność, należy zbilansować obecne podejście inwestowania w startupy:

- najpierw **kreować stabilny popyt** poprzez kierowanie zamówień publicznych **na lokalne rozwiązania**.
- następnie **budować skalę** w masowych segmentach rynku (IT, connectivity, AI, cybersecurity) na kanwie również wyzwań skierowanych do nauki i innowatorów.
- dopiero na tym fundamencie nastąpi organiczny rozwój działów **B+R i kumulacja własnego know-how (IP)**, które pozostanie w kraju tak jak w Chinach, Izraelu, Korei Południowej czy Japonii.

Wyniki badania opinii publicznej

W odpowiedzi **na pytanie o znaczenie suwerenności technologicznej naszego kraju**, jest ona postrzegana jako kwestia priorytetowa – **56% Polaków uważa, że ma ona duże (33%) lub bardzo duże (23%) znaczenie**. Zaledwie 9% respondentów marginalizuje ten temat, przypisując mu małą wagę. Jednocześnie aż 35% badanych nie ma sprecyzowanej opinii ("trudno powiedzieć"), co wskazuje, że dla jednej trzeciej społeczeństwa pojęcie to pozostaje jeszcze dość abstrakcyjne.

Pytani o to, **o ile wyższą cenę za polskie lub europejskie technologie są gotowi zaakceptować, Polacy wykazują wysoką gotowość do poniesienia tzw. "premii za suwerenność".** Aż **71% badanych jest skłonnych zapłacić więcej za rodzime rozwiązania**, przy czym główną barierą psychologiczną pozostaje próg 10%, który akceptuje 40% ankietowanych. Dopłatę rzędu 11-20% deklaruje 21% osób, a wyższe podwyżki (powyżej 20%) akceptuje jedynie co dziesiąty badany. Zdecydowany sprzeciw wobec jakichkolwiek dopłat wyraża 29% społeczeństwa. Gotowość do wsparcia finansowego jest silnie skorelowana z wiekiem oraz statusem materialnym – największymi ambasadorami takich rozwiązań są ludzie młodzi (w grupie do 24 lat aż 51% dopłaciłoby ponad 10%) oraz osoby najzamożniejsze, wśród których zaledwie 4% odmawia poniesienia wyższych kosztów (w kontraście do aż 46% odmów w grupie najuboższej).

W kwestii **zaufania do technologii, produktów i usług, blisko połowa społeczeństwa (45%) deklaruje, że polski lub europejski kapitał w infrastrukturze krytycznej i e-usługach zwiększa ich poczucie bezpieczeństwa**. Dla 41% badanych pochodzenie rozwiązań pozostaje całkowicie bez wpływu, a zaledwie 14% deklaruje spadek zaufania do lokalnych dostawców. O ile wiek nie odgrywa w tym przypadku większej roli, kluczowymi czynnikami budującymi zaufanie do rodzimego kapitału są wykształcenie, zamożność i wielkość ośrodka zamieszkania. Najwyższy poziom ufności wobec lokalnych firm wykazują przede wszystkim osoby o bardzo dobrej sytuacji finansowej (68%), z wyższym wykształceniem (56%) oraz mieszkańcy największych metropolii (54%), podczas gdy osoby z wykształceniem zawodowym pozostają w większości (52%) wobec tego faktu obojętne.

W odpowiedzi **na pytanie o zagrożenia motywujące do zapewnienia suwerenności technologicznej, Polacy wskazują przede wszystkim na namacalne, fizyczne skutki braku niezależności**. Najważniejsze obawy społeczeństwa to **zdalne wyłączenie infrastruktury krytycznej przez obcego producenta (51%), szpiegostwo i inwigilacja przez pozaeuropejskie służby (48%), odcięcie dostaw elektroniki w razie kryzysu (45%) oraz presja polityczna ze strony państw trzecich (44%)**. Z kolei zagrożenia czysto wirtualne, takie jak ukryte podatności na cyberataki, budzą znacznie mniejszy niepokój, plasując się na końcu zestawienia (29%). Chociaż ogół społeczeństwa racjonalnie ocenia te ryzyka, zauważalne są pewne różnice: mężczyźni i osoby starsze lub lepiej wykształcone częściej obawiają się twardych skutków gospodarczych oraz paraliżu infrastruktury, kobiety zwracają większą uwagę na ryzyka społeczne i informacyjne (dezinformacja, presja polityczna), a najmłodsi badani najbardziej niepokoją się wizją odcięcia dostaw sprzętu (59%).

Oceniając **gotowość Polski na wyzwania suwerenności technologicznej, zaledwie 24% badanych wierzy, że państwo jest przygotowane do ochrony swojej niezależności w tym obszarze**, przy czym tylko 4% wyraża w tej kwestii pełne przekonanie. Znacznie większa grupa (34%) ocenia stopień przygotowania kraju negatywnie, a dominująca większość – aż 42% respondentów – nie potrafi zająć jednoznacznego stanowiska, co dowodzi, że stan zaplecza technologicznego i cyberbezpieczeństwa jest dla ogółu obywateli tematem niejasnym lub zbyt abstrakcyjnym. Najbardziej krytyczni w swoich ocenach są mężczyźni oraz osoby z wyższym wykształceniem (44% negatywnych wskazań), natomiast największy optymizm (37% ocen pozytywnych) deklarują osoby o najwyższym statusie materialnym. Brak wiedzy na ten temat jest szczególnie widoczny wśród osób z wykształceniem podstawowym, gdzie rekordowe 55% badanych wybrało odpowiedź „trudno powiedzieć”.

...

W kwestii **kierunków rozwoju suwerenności technologicznej, 57% Polaków opowiada się za modelem „Twierdzy Europa", postulując budowę niezależności wyłącznie w oparciu o własne zasoby krajowe (29%) lub współpracę ograniczoną do struktur Unii Europejskiej (28%)**. Mniejsza, choć nadal znacząca grupa (43%), preferuje model mieszany, zakładający łączenie potencjału UE z sojuszami z zaufanymi krajami trzecimi, takimi jak USA, Japonia czy Korea Południowa. Wizja unijno-narodowej samowystarczalności dominuje przede wszystkim wśród osób w średnim wieku (65% w grupie 35-44 lata) oraz mieszkańców wsi (61%). Z kolei otwarcie na szerokie sojusze globalne jest domeną osób z wyższym wykształceniem (53%) oraz respondentów o najwyższym statusie materialnym (50%), którzy rzadziej wierzą w możliwość osiągnięcia pełnej niezależności bez udziału światowych potęg technologicznych.

W kwestii **działań mających na celu zwiększenie autonomii Unii Europejskiej, polskie społeczeństwo zdecydowanie preferuje mechanizmy stymulacyjne i rozwojowe („marchewkę") nad twardym protekcjonizmem i zakazami („kijem")**. Największym poparciem cieszą się programy pomocowe i dotacje na badania oraz rozwój technologii krytycznych (55%), zaostrzenie kar dla platform społecznościowych za dezinformację (54%) oraz wprowadzenie wymogu posiadania europejskich certyfikatów cyberbezpieczeństwa (53%). Najmniejszy entuzjazm budzą natomiast sztuczne ingerencje rynkowe, takie jak nakładanie nowych ceł (38%), uzależnianie dostępu do funduszy unijnych od wykorzystania lokalnych technologii (36%) czy wprowadzanie minimalnych budżetów zakupowych wyłącznie dla europejskich producentów (35%). Analiza postaw pokazuje, że podczas gdy mężczyźni wykazują większą skłonność do popierania twardych interwencji państwowych, poparcie dla systemowych regulacji bezpieczeństwa drastycznie rośnie wraz z wiekiem oraz poziomem wykształcenia respondentów, osiągając 65% w grupie osób po studiach wyższych.

Analiza działań wybranych państw w zakresie suwerenności technologicznej

Dokonano analizy działań dziewięciu krajów: Brazylii, Chin, Danii, Francji, Indii, Izraela, Japonii, Korei południowej, i Niemiec z punktu widzenia suwerenności technologicznej. Analiza została przeprowadzona według ustrukturyzowanego schematu, który pozwala na systematyczne porównanie obranych strategii.
Przegląd opiera się na następujących kategoriach:

- **kluczowe filary i wizja suwerenności** - główne doktryny i filozofia działania (np. brazylijska „względna autonomia", chińska doktryna „samowystarczalności" i „podwójnego obiegu", indyjska koncepcja *Atmanirbhar Bharat* czy francuska *Souveraineté Numérique*).
- **koordynacja polityk, instytucje i wdrożenia** - architektura decyzyjności, czyli wyznaczanie głównych ministerstw i niezależnych, wyspecjalizowanych agencji ds. cyfryzacji i cyberbezpieczeństwa.
- **finansowanie, strategie i ulgi** - narzędzia wsparcia w postaci budżetów, państwowych funduszy kapitałowych (VC), systemów ulg podatkowych oraz bezpośrednich programów dotacyjnych na rozwój (B+R).
- **preferencje dla lokalnych firm i zamówienia publiczne** - mechanizmy miękkiego protekcjonizmu, wymogi „local content", oraz rygorystyczne systemy certyfikacji faworyzujące rodzimych dostawców.
- **współpraca z rynkiem** - modele tworzenia krajowych czempionów, partnerstwa publiczno-prywatne (PPP) oraz budowa darmowej, państwowej infrastruktury bazowej (ang. *public rails*) wspierającej prywatne innowacje.
- **dyplomacja technologiczna i eksport** - wykorzystywanie osiągnięć cyfrowych jako geopolitycznego narzędzia *soft power* i budowania wpływów na świecie.
- **kluczowe technologie i sektory** - priorytetowe obszary koncentracji inwestycji, w tym: suwerenna sztuczna inteligencja (AI), powrót produkcji półprzewodników, chmury rządowe, oprogramowanie *open source* i technologie kwantowe.

Co robią państwa, by zwiększyć suwerenność?

Z przeglądu działań wyłaniają się wyraźne globalne trendy. Wiodące gospodarki opierają swoją suwerenność technologiczną na kilku spójnych filarach:

- **powrót do polityki przemysłowej i potężne zastrzyki kapitału** - państwa przestały wierzyć w samoregulację i kierują dziesiątki miliardów dolarów w strategiczne gałęzie technologii. Wykorzystują w tym celu innowacyjne mechanizmy – od bezpośrednich grantów gotówkowych pokrywających większość kosztów trudnych projektów (Izrael), przez lewarowanie i mobilizację gigantycznego kapitału prywatnego do wsparcia lokalnych funduszy (francuski Plan Tibi), po subsydia uzależnione od rzeczywistego wzrostu fizycznej produkcji na terytorium kraju (indyjski system PLI).
- **zamówienia publiczne i miękki protekcjonizm jako tarcza ochronna** - zamówienia publiczne i local content stały się świadomym narzędziem stymulowania innowacji. Kraje stosują system marż preferencyjnych, by móc legalnie kupować droższe, ale tworzone w kraju rozwiązania. Dodatkowo państwa tworzą bardzo wyśrubowane systemy certyfikacji bezpieczeństwa (np. francuski standard SecNumCloud, koreański CSAP czy japoński ISMAP), które de facto stanowią barierę wejścia dla zagranicznego big techu i oddają lukratywny rynek publiczny w ręce lokalnych dostawców.
- **budowa suwerennej chmury i rygorystyczna ochrona danych** - fundamentalnym trendem jest odzyskiwanie kontroli nad miejscem i mechanizmami przechowywania danych obywateli przedsiębiorców i administracji. Wiele krajów prawnie wymusza ich lokalizację wewnątrz swoich granic (np. Brazylia, Korea Płd., Japonia, Chiny). Ponadto, tworzone są specjalne „suwerenne chmury" rządowe, w ramach których amerykańscy dostawcy (np. Microsoft czy AWS) często zmuszeni są zawierać *joint venture* z firmami lokalnymi, które jako jedyne posiadają operacyjny dostęp i klucze szyfrujące (model francuski czy brazylijski). Istnieją też chmury całkowicie oparte o krajowe rozwiązania co generuje IP i większy know-how.

...

...

- **odejście od korporacyjnych monopoli dzięki technologiom *open source*** - kraje, takie jak Dania, Francja i Niemcy, dostrzegły zagrożenie w pułapce „vendor lock-in". Państwa te systemowo wypierają amerykańskie i zagraniczne licencje (np. pakiety biurowe czy komunikatory) ze swojej administracji, odgórnie narzucając i współtworząc rozwiązania *open source* (otwarto źródłowe). Zapewnia to transparentność kodu, niezależność od woli dostawców i ostatecznie wielomiliardowe oszczędności.
- **suwerenne AI i powrót produkcji półprzewodników** - aby uniknąć postępującej kolonizacji kulturowej, cyfrowej i mediatyzacji polityki, rządy nie chcą opierać swoich gospodarek na zachodnich platformach sztucznej inteligencji. Finansują rozwój narodowych, otwartych modeli LLM uczonych lokalnego języka i kultury (Japonia, Francja, Brazylia, Indie). Jednocześnie niemal każdy z analizowanych krajów wdrożył dotowane gigantycznymi kwotami ustawy wspierające reindustrializację i odbudowę łańcuchów dostaw półprzewodników u siebie. Szereg krajów podejmuje też działania z zakresu ograniczenia wpływu mediów społecznościowych i większej ochrony dzieci i młodzieży.
- **dyplomacja technologiczna (TechPlomacy)** - sukcesy technologiczne przekuwane są na instrumenty geopolityki i dyplomacji. Chiny uzależniają Globalne Południe swoimi technologiami poprzez „Cyfrowy Jedwabny Szlak", Indie masowo eksportują swoją darmową infrastrukturę płatniczą (UPI/DPI) by budować sojusze, Dania powołała Ambasadora Technologicznego negocjującego z korporacjami jak z obcymi mocarstwami, a Izrael wykorzystuje zaawansowane systemy bezpieczeństwa jako walutę stabilizującą relacje z sojusznikami oferując ich np. systemy do szpiegowania i ataków w sferze cyber.
- **ochrona infrastruktury i fuzja cywilno-wojskowa** - w wielu krajach (zwłaszcza w Japonii, Chinach, Korei czy Francji) po cichu odbywają się czystki sprzętowe – prawne wymuszanie na operatorach telekomunikacyjnych czy instytucjach usunięcia niepożądanego zagranicznego sprzętu w celu minimalizacji ryzyka wyłączeń lub szpiegostwa. Z kolei w państwach operujących w ciągłym zagrożeniu (Izrael, Chiny), suwerenność opiera się na transferze innowacji wojskowych do cywilnego biznesu, co pozwala osiągnąć dominację w technologiach *deep tech* i obronnych.

WPROWADZENIE

W dobie gwałtownej cyfryzacji suwerenność technologiczna przestała być wyłącznie teoretycznym konceptem badawczym, a stała się realnym fundamentem bezpieczeństwa i konkurencyjności europejskiej gospodarki. Niniejszy raport zaprasza do pogłębionej refleksji nad stanem naszej zależności w świecie zdominowanym przez globalnych gigantów technologicznych. To syntetyczne podsumowanie badania opinii społecznej na temat suwerenności technologicznej ale też przyczyn i skutków utraty suwerenności oraz możliwych rozwiązań.

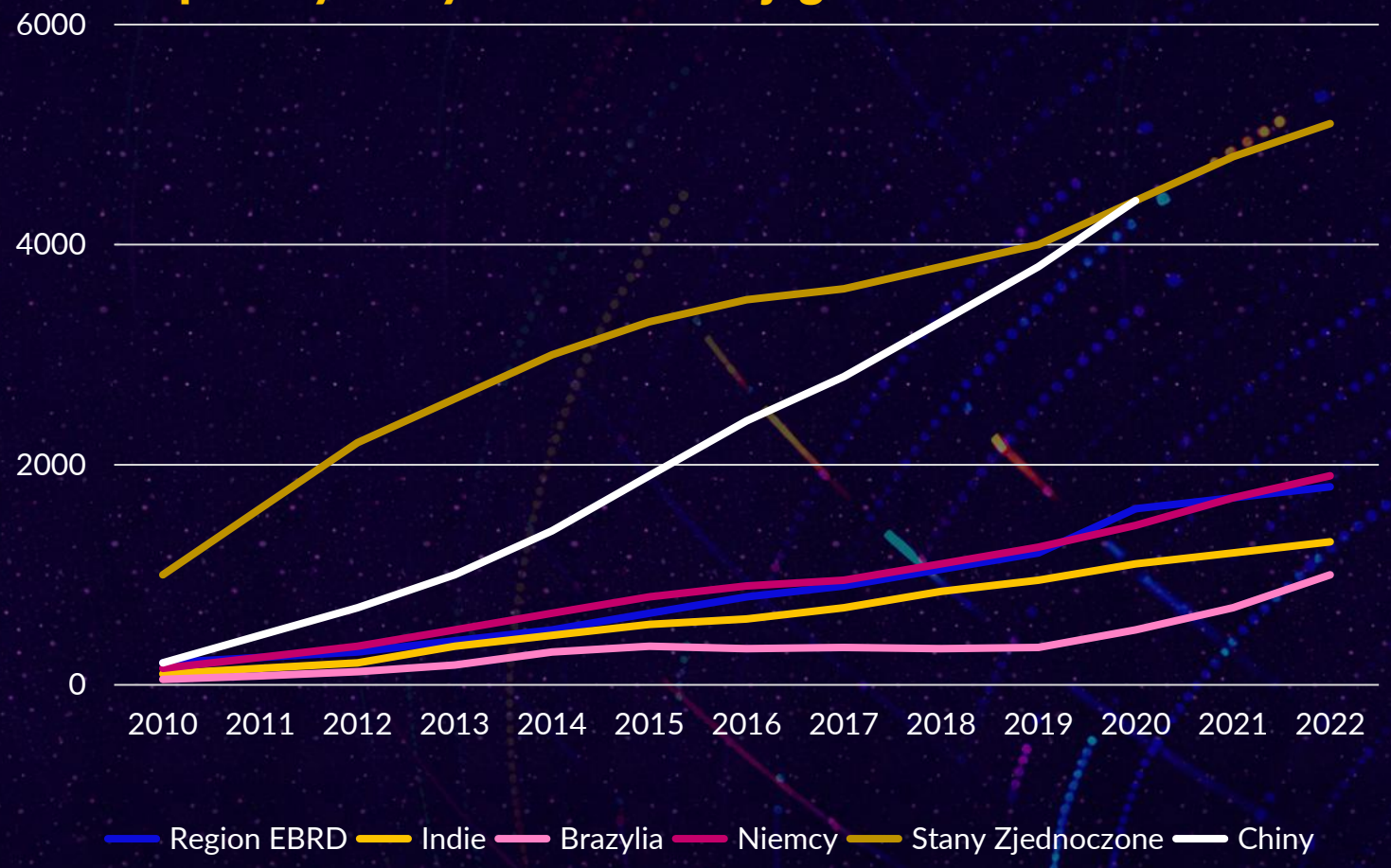
Anatomia utraty suwerenności technologicznej czyli jak do tego doprowadziliśmy

- **Brak równych warunków dla wymiany handlowej i gospodarczej**
  otwarte granice UE vs. asymetryczne bariery (np. lokalne certyfikaty i pozwolenia) oraz zamknięte zamówienia publiczne np. w Azji.
- **Błędne założenie dotyczące braku skutków przeniesienia produkcji do Azji**
  skutkowało to utratą know-how, a „inżynier" utracił dostęp do fabryki i problemów, które można rozwiązać.
- **Nieskuteczne lokalne prawo antymonopolowe**
  kary dla big tech i monopoli jako zwykły koszt prowadzenia biznesu.
- **Stworzenie warunków prawnych dla utracenia suwerenności poprzez dofinansowanie dostępu do klientów bez budowy własnych rozwiązań**
  brak tzw. *fair share* w telekomunikacji i koncentracja na promocji kompetencji cyfrowych przy braku skalowania europejskich rozwiązań.
- **Triumf pozaeuropejskiego lobbingu nad dialogiem**
  mediatyzacja polityki w wyniku rozwoju AI, wzrost istotności zasięgów w social media, kręcenia „rolek" przez polityków, które wypierają głos samorządu gospodarczego i działania w oparciu o wiedzę.
- **Pułapka „darmowych" produktów i usług**
  oddanie najcenniejszych danych przedsiębiorców i konsumentów globalnym platformom co było podstawą stworzenia AI oraz nowych produktów.
- **Wizje gospodarcze UE bez tarczy przemysłowej**
  różne polityki, w tym zielony ład, de facto otwierały UE na azjatycki import przy braku local content i odpowiedników typu Build America, Buy America czy Made in China.
- **Fuzja technologii czyli technologie podwójnego zastosowania, które napędzają big tech**
  AI i technologie cywilne są narzędziem geostrategicznej kontroli rynków i społeczeństw. Poszatkowany rynek europejskich zamówień dla wojska skutkował skierowaniem zamówień poza Europę. Big tech był beneficjentem.
- **Drenaż europejskiego kapitału i „samo sprzedawanie się"**
  brak jednolitego rynku kapitałowego sprawił, że UE eksportuje swoje oszczędności do USA i finansuje amerykańskie platformy (np. chmurę i AI) wypierając własne europejskie rozwiązania. Platformy dekadami subsydiują dostęp do własnych produktów oferując je „za darmo" by zniszczyć konkurencję.
- **Grzech biznesu jako skupienie się na „tu i teraz"**
  zamiast stawiania na wiedzę, trwałą suwerenność i długoterminowy rozwój, wybrano krótkoterminowe zyski.

Cena zależności czyli jak brak suwerenności technologicznej uderza w krajowe firmy

- **Niewiele suwerenności to niewielkie zyski!!!**
  biznes technologiczny i cyfrowy w suwerennych krajach generuje 25-35% marże, podczas gdy w UE marże firm spadają do 5-10% jako głównie biorców rozwiązań.
- **Gigantyczny deficyt handlowy to miejsce na szantaże**
  wg Sieci Badawczej Łukasiewicz mamy ok. 45 mld PLN deficyt handlowy w usługach cyfrowych. Poziom uzależnienia zaczyna swoją skalą przypominać historyczną skalę naszego uzależnienia od paliw kopalnych z Rosji.
- **Asymetria i zabójcze koszty zgodności z prawem**
  krajowe MŚP są dławione regulacjami, podczas gdy giganci spoza Europy korzystają z dotacji/subwencji i luźniejszych regulacji u siebie.
- **Szklany sufit w przetargach dla krajowych firm**
  dyskryminacja polskich firm w przetargach (np. na laptopy, chmura, AI) i pisanie ich pod dyktando globalnych marek. Polska jest liderem w UE w ustawionych przetargach. Aż 53,6% przetargów w 2025 roku miało tylko jednego oferenta, a bardzo często SIWZ sugerował tylko jedną firmę by nikt inny nie wystartował.
- **Koszty rozwoju sieci bez znacznych zysków**
  sektor telekomunikacyjny finansuje darmowe cyfrowe autostrady dla pozaeuropejskich usług cyfrowych i produktów gigantów.
- **Syndrom najemcy, ryzyko paraliżu i „kill switch”**
  ryzyko odcięcia państwa i naszych firm od usług (przykłady: łączność satelitarna w Ukrainie, pakiet biurowy w MTK w Hadze).
- **Zagrożenie bezpieczeństwa państwa**
  utrata zdolności do obrony państwa, firm i ochrony obywateli przy technologii kontrolowanej i rozwijanej z zewnątrz.
- **Paraliż operacyjny i produkcyjny**
  ryzyko natychmiastowych przestojów przez brak krytycznych komponentów (np. półprzewodników, GPU, metali ziem rzadki, API).
- **Szpiegostwo i drenaż know-how**
  utrata kontroli nad wrażliwymi danymi i IP (lekcja z afery Snowdena).
- **Neuronowa (AI) manipulacja demokracją**
  nieprzewidywalny i negatywny wpływ pozaeuropejskich platform na wybory, marginalizacja merytorycznego stanowienia prawa w dialogu z firmami oraz poważne problemy tradycyjnych, niezależnych mediów.
- **Mediatyzacja polityki i marginalizacja prawnego procesu stanowienia prawa**
  zasięgi i „rolki” wypierają głos samorządu gospodarczego w procesie legislacyjnym. Urzędnicy przy tym tracą atencję rządzących. Następuje degrengolada całego procesu stanowienia prawa.

Od 2019 roku liczba realizowanych polityk przemysłowych i interwencji gwałtownie wzrosła



Współczesna gospodarka globalna przechodzi fundamentalną transformację – era „niewidzialnej ręki rynku" ustępuje miejsca bardzo wyraźnej interwencji państwowej. Jak wskazują analizy (m.in. EBRD), od 2019 roku obserwujemy bezprecedensowy renesans polityki przemysłowej, widoczny zarówno w mocarstwach, jak i na rynkach wschodzących. Ten zwrot nie wynika z ideologii, lecz z twardej konieczności: rosnącej fragmentacji geopolitycznej, potrzeby zabezpieczenia łańcuchów dostaw oraz faktu, że inne kraje agresywnie dotują własnych czempionów. W takim otoczeniu bierność Polski staje się strategią wysokiego ryzyka, grożącą marginalizacją rodzimych firm. Kluczem nie jest jednak bezkrytyczne kopiowanie starych wzorców, lecz budowa nowoczesnej sprawności administracyjnej. Skuteczny interwencjonizm wymaga precyzyjnych narzędzi – wspierania B+R i eksportu zamiast prostego protekcjonizmu – oraz stosowania tzw. klauzul wygasania (sunset clauses), które zapobiegają uzależnieniu przedsiębiorstw od państwowej kroplówki. Polska musi przestać być jedynie rynkiem zbytu dla dotowanych technologii z zewnątrz i stać się aktywnym architektem własnej odporności przemysłowej, łącząc kapitał publiczny z rygorem rynkowej konkurencyjności.

B+R w służbie suwerenności - dlaczego innowacje wymagają skali i produkcji?

Innowacja jako pochodna produkcji, a nie jej poprzednik

W sektorach wysokich technologii, takich jak półprzewodniki, panuje błędne przekonanie, że same inwestycje w badania i startupy wystarczą do zbudowania przewagi technologicznej. Historia globalnych liderów – Japonii, Korei Południowej czy Tajwanu – dowodzi czegoś odwrotnego: przełomy w B+R zawsze rosły przy liniach produkcyjnych, a nie w izolacji od nich. Innowacje procesowe rodzą się tam, gdzie istnieje realny wolumen produkcji, pozwalający na rozwiązywanie konkretnych problemów z wydajnością, uzyskiem i kosztami. Bez własnej produkcji innowacja pozostaje jedynie teoretyczną koncepcją, a nie trwałą kompetencją narodu.

Pułapka świetnego startupu i iluzja grantów dla gigantów

Brak wsparcia dla budowy skali produkcji sprawia, że nawet najlepiej dofinansowane europejskie projekty B+R trafiają w próżnię. Gdy przychodzi etap komercjalizacji, małe firmy albo upadają, albo są przejmowane przez zagraniczne koncerny, co skutkuje utratą własności intelektualnej (IP) sfinansowanej z publicznych środków. Podobne ryzyko niesie opieranie suwerenności wyłącznie na grantach dla zagranicznych gigantów – przykład wstrzymania inwestycji Intela pod Wrocławiem pokazuje, że jeśli IP i decyzje strategiczne pozostają poza krajem, fizyczna fabryka nie daje realnej kontroli ani odporności na kryzysy.

Strategiczna kolejność działań - popyt jako paliwo dla innowacji

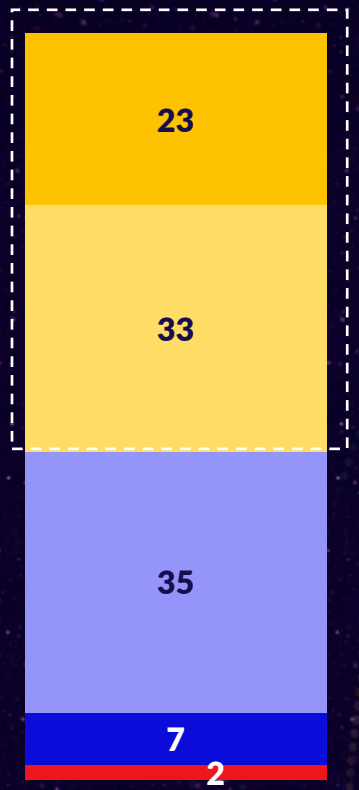
Aby B+R stało się narzędziem realnej suwerenności, polityka przemysłowa musi odwrócić dotychczasowe priorytety i działać według pragmatycznego modelu:

- kreowanie popytu - fundamentem jest systemowe przesunięcie zamówień publicznych i zakupów dużych spółek na lokalne rozwiązania. To stabilny popyt pozwala polskim firmom planować inwestycje i rozwijać kompetencje.
- budowa skali w całym łańcuchu - koncentracja na wąskich „aplikacjach krytycznych” (5% rynku) to błąd. Skala musi powstawać w masowych segmentach np. takich jak IT, connectivity, AI, cybersecurity.
- naturalny rozwój własnego IP –dopiero na fundamencie skali następuje organiczny rozwój działów B+R i kumulacja autorskiego know-how, które zostaje w kraju.

Prawdziwa suwerenność technologiczna nie zaczyna się od deklaracji, lecz od posiadania masy krytycznej w produkcji, która pozwala stabilizować łańcuchy dostaw i przeciwdziałać potencjalnym szantażom technologicznym.

BADANIE OPINII PUBLICZNEJ

Jakie znaczenie ma dla Ciebie suwerenność technologiczna naszego kraju?



Dla ponad połowy badanych (56%) suwerenność technologiczna Polski ma duże znaczenie. Marginalna część respondentów deprecjonuje wagę tego zjawiska. Zaledwie 9% uważa je za mało istotne.

Suwerenność technologiczna jest postrzegana jako ważna głównie przez osoby starsze, lepiej wykształcone, mężczyzn oraz osoby o wyższym statusie materialnym. Wyzwaniem pozostaje natomiast edukacja w tym zakresie osób młodszych oraz tych z niższym wykształceniem, wśród których dominuje brak sprecyzowanej opinii.

ⓘ Pytanie jednowyborowe. Podstawa: wszyscy respondenci, N=1000 Polaków w wieku 16-75 lat

Jakie znaczenie ma dla Ciebie suwerenność technologiczna naszego kraju?

Segmentacja

W ogólnym przekroju, dla ponad połowy badanych (56%) suwerenność technologiczna Polski ma duże znaczenie, z czego 33% określa je jako „duże", a 23% jako „bardzo duże". Marginalna część respondentów deprecjonuje wagę tego zjawiska – zaledwie 9% uważa je za mało istotne (7% przypisuje mu „małe" znaczenie, a 2% „bardzo małe"). Uwagę zwraca stosunkowo wysoki odsetek osób nieposiadających wyrobionego zdania - 35% Polaków wybrało odpowiedź „trudno powiedzieć", co może sugerować, że pojęcie to dla 1/3 części społeczeństwa pozostaje jeszcze nieco abstrakcyjne lub niezrozumiałe.

Kwestia suwerenności technologicznej wyraźnie różnicuje badanych ze względu na płeć. Mężczyźni znacznie częściej deklarują, że jest to dla nich ważny temat – uważa tak 60% z nich (w tym 28% wskazuje na znaczenie „bardzo duże"). Z kolei wśród kobiet wskaźnik ten wynosi 52%, przy czym panie znacznie częściej mają problem z jednoznaczną oceną sytuacji (38% odpowiedzi „trudno powiedzieć" w stosunku do 31% wśród mężczyzn).

Dostrzegalna jest również zależność związana z wiekiem – waga przypisywana niezależności technologicznej nieznacznie rośnie wraz z wiekiem respondentów. Podczas gdy w najmłodszej grupie (poniżej 24 lat) istotność tego zagadnienia podkreśla 53% badanych, wśród osób powyżej 55. roku życia odsetek ten rośnie do 61%. Najmłodsi stosunkowo najczęściej (21%) wskazują na małe lub bardzo małe znaczenie tego aspektu.

Kluczowym czynnikiem wpływającym na świadomość w tym zakresie okazuje się wykształcenie i status społeczno-ekonomiczny. Niezależność technologiczna kraju jest priorytetem przede wszystkim dla osób z wykształceniem średnim i wyższym – w obu tych grupach aż 66% badanych ocenia jej znaczenie jako duże lub bardzo duże. Dla kontrastu, wśród osób z wykształceniem zasadniczym zawodowym wskaźnik ten wynosi zaledwie 38%, a ponad połowa tej grupy (51%) nie potrafi zająć stanowiska w tej sprawie. Podobnie najwyższą świadomość wagi suwerenności (wynik na poziomie aż 76% odpowiedzi twierdzących) odnotowano wśród osób deklarujących bardzo dobrą sytuację finansową i standard życia wyższy niż przeciętny oraz pracujących na wyższych stanowiskach umysłowych.

Maciej Wyczesany

Prezes Zarządu Apator S.A.

Suwerenność technologiczna jako fundament bezpieczeństwa energetycznego

W dobie cyfrowej transformacji sieci energetycznych, bezpieczeństwo kraju przestaje być wyłącznie kwestią miksu energetycznego, a staje się wyzwaniem z obszaru cyberbezpieczeństwa. Apator od dłuższego czasu konsekwentnie podnosi alarm: polska sieć energetyczna, w której zainstalowano miliony urządzeń IoT (m.in. inwertery fotowoltaiczne, sterowniki, liczniki), jest dziś realnie zagrożona „technologiczną kolonizacją" ze strony dostawców z krajów trzecich, głównie z Azji.

Ryzyko zdalnego wyłączenia i "bezpieczne" liczniki

Z naszej perspektywy liczniki energii ze zdalnym odczytem – które są elementem infrastruktury krytycznej – to nie tylko urządzenia pomiarowe, ale ważne „punkty komunikacyjne", które mogą służyć do destabilizacji systemu. Ryzyko zdalnego wyłączenia zasilania jest prawdopodobne, ponieważ urządzenia te działają w oparciu o oprogramowanie, do którego kody źródłowe pozostają pod kontrolą podmiotów funkcjonujących poza krajową jurysdykcją, potencjalnie podatnych na naciski polityczne.

Apator adresuje te obawy, stawiając na pełną kontrolę łańcucha dostaw i „security by design". Jako polski producent, oferujemy rozwiązania, których kod źródłowy powstaje w kraju, a procesy produkcyjne są transparentne i audytowalne. Obserwujemy wzrost zainteresowania bezpiecznymi technologiami wśród spółek Skarbu Państwa, jednak proces ten wymaga usystematyzowania poprzez wprowadzenie wiążących norm cyberbezpieczeństwa. Powinny one obejmować wymogi dotyczące transparentności pochodzenia producenta i produktów oraz zapewnienie, że oprogramowanie urządzeń dla infrastruktury krytycznej jest rozwijane w UE zgodnie z ISO 27001 a producent podlega audytowi zamawiającego.

Sentyment konsumencki a realia przetargowe

Choć z przeprowadzonego badania wynika, że Polacy deklarują wyższe zaufanie do polskiego i europejskiego kapitału, w sektorze energetycznym to zaufanie rzadko przekłada się na twarde kryteria wyboru dostawcy. Dostrzegamy rażący dysonans: podczas gdy społeczeństwo oczekuje bezpieczeństwa, w przetargach wciąż dominuje kryterium najniższej ceny. Prowadzi to do sytuacji, w której europejscy producenci, obciążeni kosztami certyfikacji, przestrzegania norm środowiskowych i etycznych, przegrywają z silnie dotowanymi przez państwo dostawcami z Chin. W efekcie, krótkowzroczne oszczędności przy zakupie urządzeń mogą generować w przyszłości dużo wyższe koszty dla stabilności i bezpieczeństwa systemu.

Postulaty regulacyjne: jak ograniczyć zależność?

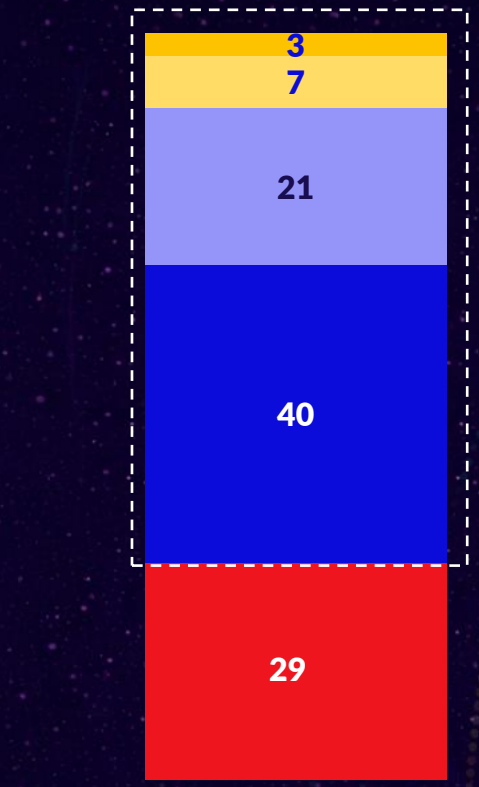
Aby uniknąć pułapki technologicznej, Apator i inni europejscy producenci postulują zmianę podejścia regulacyjnego m.in. wprowadzenie obowiązkowych badań cyberbezpieczeństwa dla wszystkich urządzeń instalowanych na sieci, stosowanie kryteriów pozacenowych w przetargach (np. wymóg posiadania serwisu, wsparcia technicznego oraz centrum rozwoju oprogramowania na terenie UE/NATO). Kluczowa jest także weryfikacja pochodzenia kapitału – powinniśmy kategorycznie uwzględniać ryzyka geopolitycznie przy ocenie dostawców dla infrastruktury krytycznej i nie pozwalać, by środki przeznaczane na zakup urządzeń dla infrastruktury krytycznej (często pochodzące z dotacji publicznych) były transferowane poza UE.

Wykorzystanie zaufania do przyspieszenia inwestycji

Branża energetyczna musi przekuć społeczne zaufanie do krajowych technologii w realną strategię gospodarczą. Stoimy na stanowisku, że państwo powinno pełnić rolę mądrego zamawiającego, który poprzez zamówienia publiczne stymuluje rozwój rodzimego przemysłu. Inwestycje w cyfryzację i automatyzację sieci są konieczne, aby zapewnić bieżące bilansowanie, przewidywalność pracy sieci oraz bezpieczeństwo dostaw energii. Jeśli system elektroenergetyczny będzie oparty na technologii kontrolowanej lokalnie (tj. w Europie), zyskamy odporność na ewentualny szantaż technologiczny, co w obecnej sytuacji geopolitycznej powinno być priorytetem.

Podsumowując, suwerenność energetyczna i gospodarcza Polski zależy dziś od tego, czy zdołamy obronić nasze sieci przed zalewem taniej, ale niezweryfikowanej pod kątem bezpieczeństwa technologii, stawiając na sprawdzonych, krajowych i europejskich partnerów.

O ile wyższą cenę za polskie lub europejskie technologie jesteś gotów zaakceptować, by wspierać naszą suwerenność?



Ponad 30% więcej
21-30% więcej
11-20% więcej
Do 10% więcej
0% - nie zapłacił(a)bym więcej

Polacy wykazują zdecydowaną gotowość (71%) do poniesienia dodatkowych kosztów w imię wsparcia suwerenności technologicznej, choć ich entuzjazm wyraźnie zależy od sytuacji materialnej, wieku i wykształcenia.

Gotowość społeczeństwa na tzw. premię za suwerenność jest wysoka, jednak dla zdecydowanej większości barierą psychologiczną pozostaje próg 10% narzutu cenowego.

Największymi ambasadorami technologicznego patriotyzmu są dziś w Polsce ludzie młodzi, wykształceni, dobrze zarabiający i dużych miast.

Pytanie jednowyborowe. Podstawa: wszyscy respondenci, N=1000 Polaków w wieku 16-75 lat
Pytanie: Jeśli okazałoby się, że koszty wytworzenia i dostarczenia europejskiej technologii są wyższe niż globalnych dostawców, o ile wyższą cenę zaakceptował(a)by Pan(i) za produkty, usługi i technologie wytwarzane w Polsce lub w Unii Europejskiej w celu wspierania suwerenności technologicznej?

O ile wyższą cenę za polskie lub europejskie technologie jesteś gotów zaakceptować, by wspierać naszą suwerenność?

Segmentacja

W ogólnym przekroju, znakomita większość badanych, aż 71%, deklaruje, że mogłaby zaakceptować wyższą cenę za produkty, usługi i technologie wytwarzane w Polsce lub na terenie Unii Europejskiej w stosunku do globalnych dostawców. Najczęściej wskazywanym, akceptowalnym progiem podwyżki jest dopłata w wysokości do 10%, co stanowi granicę tolerancji dla 40% ankietowanych. Co piąty respondent (21%) jest skłonny ponieść koszt o 11–20% wyższy, a co dziesiąty wykazuje bardzo wysoki poziom zaangażowania, akceptując ceny wyższe o ponad 20% (w tym 7% osób godzi się na dopłatę w przedziale 21–30%, a 3% nawet powyżej 30%). Zdecydowany brak zgody na jakiekolwiek dopłacanie do lokalnych technologii wyraża zaledwie 29% społeczeństwa.

Kwestia akceptacji wyższych cen najmocniej różnicuje się pod względem wieku. Zdecydowanymi liderami wsparcia dla europejskiej technologii są ludzie młodzi. W grupie osób poniżej 24. roku życia oraz w przedziale 25–34 lata jedynie niespełna co piąta osoba (odpowiednio 18% i 19%) odmawia poniesienia dodatkowych kosztów. Młodzi są także najbardziej hojni – w grupie do 24 lat aż 51% ankietowanych deklaruje gotowość zapłacenia za lokalne rozwiązania o ponad 10% więcej. Starsze osoby wykazują znacznie większą zachowawczość finansową. Wśród badanych powyżej 35. roku życia odsetek osób, które w ogóle nie chciałyby dopłacać w imię suwerenności, utrzymuje się na stałym, wyraźnie wyższym poziomie (od 32% do 35%).

Analiza statusu materialnego ujawnia spodziewaną, lecz bardzo silną korelację: skłonność do dopłacania za technologie rośnie proporcjonalnie do zasobności portfela. Wśród osób oceniających swoją sytuację finansową jako bardzo dobrą, zaledwie 4% respondentów nie wykazuje chęci wsparcia poprzez wyższą cenę, a aż 44% z nich gotowych jest na dopłatę przekraczającą 10%. Z drugiej strony, barierą w budowaniu niezależności technologicznej drogą konsumenckich wyborów stają się obiektywne ograniczenia budżetowe. W grupie osób, którym trudno związać koniec z końcem, odsetek odmawiających dopłat wzrasta do 39%, a wśród tych, którym wystarcza jedynie na podstawowe potrzeby, osiąga niemal połowę (46%).

Widoczne są również różnice na poziomie wykształcenia – osoby z dyplomem wyższej uczelni znacznie rzadziej odrzucają możliwość dopłaty do europejskich technologii (19% odmów) w porównaniu z osobami po szkołach zawodowych (39%). Płeć ma tutaj jedynie drugorzędne znaczenie, choć mężczyźni wykazują się minimalnie większą elastycznością cenową (tylko 27% by nie dopłaciło) w stosunku do kobiet (30%). Podobne różnice widać ze względu na lokalizację. Osoby mieszkające na wsi są mniej skłonne zapłacić więcej (34% wskazuje na 0%), niż osoby z dużych miast (27%).

Cristina Caffarra

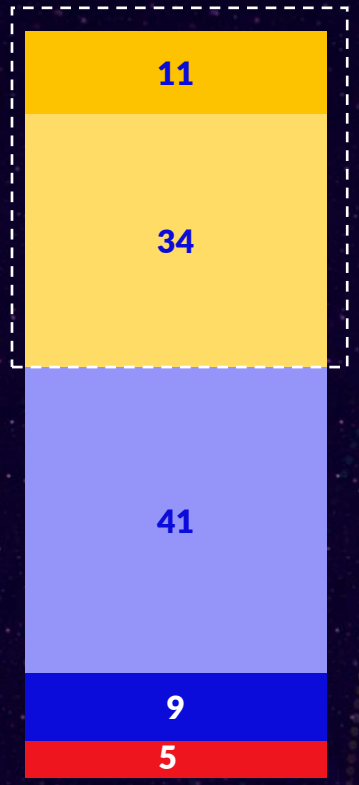
Founder and Chair, EuroStack Initiative Foundation

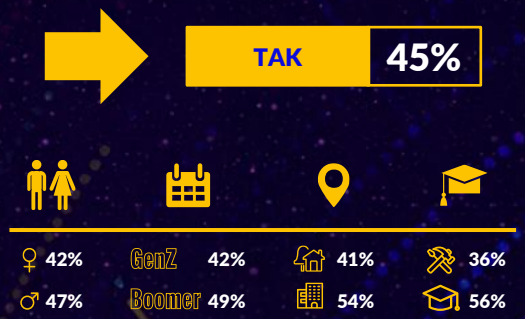
Te wyniki są zarówno budujące, jak i wcale mnie nie dziwią. Są budujące, ponieważ pokazują, że Polacy w pełni rozumieją konieczność rozwoju silnego przemysłu technologicznego w Europie oraz zmniejszenia naszych zależności od zewnętrznych aktorów. Nie są zaś zaskakujące, ponieważ podobne nastroje wybrzmiewają w całej Europie, a Polska może pochwalić się jednym z najbardziej prężnych ekosystemów technologicznych na naszym kontynencie. To właśnie jest misja EuroStack.

Jak dobitnie pokazuje raport, ponad połowa Polaków (56%) uznaje suwerenność technologiczną swojego kraju za kwestię bardzo ważną lub ważną. Niezwykle istotne jest to, że nie mówimy tu wyłącznie o pustych deklaracjach – w sytuacji, gdyby technologie wytwarzane w Europie były droższe niż rozwiązania globalnych dostawców, aż 71% Polaków byłoby skłonnych zaakceptować wyższą cenę produktów i usług w celu wspierania naszej suwerenności technologicznej. To jasny sygnał, że społeczeństwo jest gotowe na realne zaangażowanie w imię długofalowego bezpieczeństwa.

Wnioski z tego badania tylko mnie utwierdzają w przekonaniu, że nasza praca nad budową silnej, odpornej i zaawansowanej technologicznie Europy jest dziś bardziej potrzebna niż kiedykolwiek. Rozwój naszego wspólnego potencjału to już nie tylko wybór gospodarczy, to strategiczna konieczność.

Czy masz większe zaufanie do technologii, produktów i usług, jeśli stoją za nimi polskie lub europejskie firmy?





Zdecydowanie zwiększa moje zaufanie
Raczej zwiększa moje zaufanie
Nie ma to wpływu na moje zaufanie
Raczej zmniejsza moje zaufanie
Zdecydowanie zmniejsza moje zaufanie

Blisko połowa Polaków (45%) deklaruje, że opracowanie i wyprodukowanie technologii przez firmy z polskim lub europejskim kapitałem zwiększa ich zaufanie do tych rozwiązań.

Świadomość wpływu lokalnego kapitału na bezpieczeństwo e-usług i infrastruktury państwa to dziś **domena tzw. klasy wyższej,** w tym wypadku osób najlepiej wykształconych, zamożnych i mieszkających w dużych ośrodkach miejskich.

Dla ogromnej części społeczeństwa, w tym osób z niższym wykształceniem, kto stoi za daną technologią, wciąż pozostaje kwestią drugorzędną lub neutralną.

Pytanie jednowyborowe. Podstawa: wszyscy respondenci, N=1000 Polaków w wieku 16-75 lat
Pytanie: W jakim stopniu świadomość, że produkty, usługi i technologie wykorzystywane w infrastrukturze krytycznej (np. energetyce, zaopatrzeniu w wodę, sieciach telekomunikacyjnych) czy e-usługach publicznych (np. mObywatel, ePUAP, mZUS) zostały opracowane i wyprodukowane przez firmy z polskim lub europejskim kapitałem, wpływa na Pana(i) zaufanie do tych produktów, usług i technologii?

Czy masz większe zaufanie do technologii, produktów i usług, jeśli stoją za nimi polskie lub europejskie firmy?

Segmentacja

Z analizy wyników badania dotyczących wpływu pochodzenia technologii na zaufanie do infrastruktury krytycznej i e-usług publicznych płyną bardzo ciekawe, momentami wręcz nieoczywiste wnioski. Społeczeństwo jest w tej kwestii podzielone, a kluczem do zrozumienia tych różnic są kompetencje i status społeczny.

W ujęciu ogólnym, blisko połowa Polaków (45%) deklaruje, że opracowanie i wyprodukowanie technologii przez firmy z polskim lub europejskim kapitałem zwiększa ich zaufanie do tych rozwiązań (z czego 11% twierdzi tak zdecydowanie, a 34% raczej zwiększa). Dla bardzo dużej grupy, stanowiącej 41% badanych, rodowód twórców pozostaje kwestią całkowicie neutralną i nie wpływa na ich poczucie bezpieczeństwa. Jedynie mniejszość (14%) wskazuje na odwrotną korelację, czyli spadek zaufania w przypadku rozwiązań lokalnych.

Głębsze spojrzenie w dane demograficzne pokazuje delikatne różnice w postrzeganiu tego zjawiska między kobietami a mężczyznami. Panowie wykazują nieco większą wrażliwość na kwestie pochodzenia kapitału – dla 47% z nich polskie lub europejskie korzenie technologii są czynnikiem budującym zaufanie (wobec 42% wśród kobiet). Panie z kolei znacznie częściej pozostają na ten aspekt obojętne (44% wskazań na brak wpływu, podczas gdy u mężczyzn wskaźnik ten wynosi 38%). Co niezwykle interesujące, sam wiek badanych nie jest tu czynnikiem w ogóle różnicującym – odsetek osób darzących większym zaufaniem lokalne technologie oscyluje wokół 43–47% równomiernie we wszystkich przedziałach wiekowych.

Prawdziwą linią podziału okazują się natomiast wykształcenie oraz zasobność portfela. Pozytywny wpływ polskiego i europejskiego kapitału na zaufanie do e-usług rośnie liniowo wraz z posiadanym wykształceniem. O ile w grupie osób po studiach wyższych odsetek ten wynosi aż 56%, o tyle wśród badanych z wykształceniem zasadniczym zawodowym to zaledwie 32% (tu ponad połowa, bo aż 52%, pozostaje w tej kwestii obojętna, a 17% deklaruje nawet mniejsze zaufanie).

Analogiczny i bardzo silny trend widać w odniesieniu do statusu finansowego. Rekordowy poziom zaufania do lokalnych rozwiązań odnotowano wśród osób deklarujących bardzo dobrą sytuację materialną i wyższy od przeciętnego standard życia – aż 68% z nich traktuje europejski lub polski rodowód technologii jako gwarancję zaufania. Na przeciwległym biegunie znajdują się osoby zmagające się z trudnościami finansowymi (odsetek zaufania spada tam do 32-35%). Zależność widać również na mapie – mieszkańcy największych metropolii (powyżej 500 tys. mieszkańców) istotnie częściej budują swoje zaufanie w oparciu o europejski kapitał (54%) niż osoby żyjące na wsi i w najmniejszych miasteczkach (odpowiednio 41% i 43%).

Maciej Kuźniar

CEO Oktawave

Suwerenność cyfrowa oznacza przede wszystkim zdolność do sprawowania kontroli nad danymi, architekturą systemów oraz kluczowymi decyzjami technologicznymi, a nie całkowitą rezygnację z globalnych technologii. W praktyce sprowadza się to do rozwoju własnych usług chmurowych w oparciu o technologie open source i otwarte standardy, które pozwalają europejskim dostawcom budować zaawansowane warstwy usługowe bez trwałego uzależnienia od jednego, zamkniętego ekosystemu. Równocześnie istotne jest zachowanie zgodności ze standardami rynkowymi przy jednoczesnym egzekwowaniu europejskich wymogów regulacyjnych, co umożliwia realną interoperacyjność oraz swobodną migrację środowisk w obu kierunkach.

Z tej perspektywy suwerenność nie oznacza izolacji, lecz świadomą kontrolę i możliwość wyboru. Organizacje powinny mieć możliwość uruchamiania i przenoszenia obciążeń pomiędzy różnymi środowiskami chmurowymi – lokalnymi i globalnymi – w zależności od wymagań regulacyjnych, bezpieczeństwa, kosztów czy dostępności konkretnych usług. Model multi-cloud, oparty na otwartych technologiach i standaryzacji, stanowi naturalne narzędzie realizacji tak rozumianej suwerenności.

W kontekście programów wsparcia i finansowania B+R oznacza to konieczność równoległych działań na dwóch poziomach. Z jednej strony Europa powinna wzmacniać rodzimych dostawców infrastruktury IaaS, zdolnych oferować usługi porównywalne pod względem jakości, bezpieczeństwa i skali z globalnymi hyperscalerami – interoperacyjność ma bowiem sens tylko wtedy, gdy na rynku istnieją konkurencyjne alternatywy. Z drugiej strony kluczowe jest inwestowanie w warstwę oprogramowania, narzędzia i usługi wspierające migrację danych, zarządzanie złożonymi środowiskami oraz egzekwowanie polityk bezpieczeństwa i zgodności regulacyjnej.

Strategia Oktawave wpisuje się w ten model zarówno poprzez rozwój własnych usług, jak i aktywny udział w inicjatywach badawczo-rozwojowych, takich jak projekt Next Gen Cloud realizowany w ramach unijnej inicjatywy IPCEI-CIS. Jej celem jest budowa zdecentralizowanej infrastruktury chmurowej w Europie, zapewniającej interoperacyjność i suwerenność cyfrową całej UE poprzez federacyjne środowiska łączące zasoby wielu dostawców. Efektem ma być wzmocnienie europejskich kompetencji w obszarze infrastruktury, bezpieczeństwa i interoperacyjności, a nie tworzenie zamkniętego ekosystemu oderwanego od globalnych standardów.

Przykładem takiego podejścia jest partnerstwo Oktawave z Google Cloud, które umożliwia projektowanie architektury wykorzystującej zaawansowane usługi globalnego dostawcy przy jednoczesnym zachowaniu kontroli nad danymi i warstwą infrastrukturalną. Kluczowe obciążenia, dane wrażliwe oraz systemy objęte wymogami regulacyjnymi mogą być utrzymywane w środowisku Oktawave, natomiast wybrane komponenty aplikacyjne lub usługi o wysokich wymaganiach skalowalności i analityki – uruchamiane w Google Cloud. Dzięki spójnym standardom architektonicznym i otwartym technologiom możliwe jest jednolite zarządzanie takim środowiskiem, z zachowaniem kontroli nad lokalizacją i dostępem do danych oraz możliwością migracji aplikacji i zasobów.

W tym ujęciu suwerenność cyfrowa nie stoi w sprzeczności z modelem multi-cloud – przeciwnie, stanowi jego logiczne rozwinięcie. To zdolność do świadomego korzystania z różnych technologii i dostawców przy zachowaniu kontroli, elastyczności i odporności biznesowej. Suwerenność cyfrowa nie jest więc alternatywą „Europa albo świat”, lecz architekturą umożliwiającą bezpieczne, kontrolowane i elastyczne funkcjonowanie w obu tych wymiarach.

Jakie są zagrożenia i ryzyka, które powinny motywować Polskę i Europę do zapewnienia suwerenności technologicznej?

Top 4

Polacy obawiają się przede wszystkim fizycznych, namacalnych skutków braku niezależności, na dalszy plan spychając zagrożenia o charakterze czysto wirtualnym. Ponad 4 na 10 badanych wskazało cztery ryzyka uznając je za najważniejsze.

Argumentacja na rzecz budowy suwerenności technologicznej trafia do Polaków najbardziej, gdy opiera się na fundamentach **twardego bezpieczeństwa narodowego** – gwarancji tego, że w sytuacji kryzysowej w naszych domach nie zabraknie prądu, łączności oraz dostępu do podstawowego sprzętu elektronicznego, a nasze dane nie trafią w ręce obcych wywiadów.

Pytanie wielokrotnego wyboru, max 5 odpowiedzi. N=1000 Polaków w wieku 16-75 lat
Pytanie: Które zagrożenia i ryzyka powinny najbardziej motywować Polskę i Unię Europejską do zapewnienia suwerenności technologicznej? Proszę zaznaczyć maksymalnie 5 najbardziej motywujących

Jakie są zagrożenia i ryzyka, które powinny motywować Polskę i Europę do zapewnienia suwerenności technologicznej?

Segmentacja

Zestawienie ryzyk stanowiących główną motywację do wzmacniania naszej suwerenności technologicznej dowodzi, że Polacy oceniają sytuację niezwykle trzeźwo i racjonalnie. Na pierwszy plan wysuwają się lęki przed dotkliwymi, bezpośrednimi konsekwencjami braku autonomii w świecie fizycznym, natomiast zagrożenia funkcjonujące wyłącznie w sferze wirtualnej budzą w społeczeństwie mniejszy niepokój.

Zdecydowanie najważniejszym motywatorem, wskazywanym przez ponad połowę badanych (51%), jest ryzyko zdalnego wyłączenia infrastruktury krytycznej, takiej jak systemy energetyczne czy łączność, przez producenta z kraju trzeciego. Na drugim miejscu plasuje się obawa przed szpiegostwem i inwigilacją ze strony pozaeuropejskich służb wywiadowczych (48%). Trzecim najpoważniejszym zagrożeniem jest ryzyko odcięcia dostaw elektroniki, np. kluczowych półprzewodników, w przypadku globalnych konfliktów czy pandemii (45%). Niewiele mniej, bo 44% respondentów, obawia się wykorzystania technologii do wywierania politycznej presji na Polskę lub UE. Co ciekawe, potencjał ukrytych podatności na cyberataki w sprzęcie lub oprogramowaniu zamyka stawkę – wskazało na to jedynie 29% badanych.

Katalog obaw wyraźnie różnicuje się w zależności od płci. Mężczyźni znacznie częściej zwracają uwagę na twarde aspekty technologiczne i gospodarcze – mocniej obawiają się wyłączenia infrastruktury (56% wobec 47% u kobiet), odcięcia dostaw sprzętu (51% wobec 39%) czy transferu zysków poza Europę. Z kolei kobiety wykazują wyższą wrażliwość na zagrożenia o charakterze społecznym i informacyjnym, częściej wskazując na ryzyko wywierania presji politycznej i rozsiewania dezinformacji (47% wobec 41% u mężczyzn) oraz destrukcyjny wpływ pozaeuropejskich mediów społecznościowych na procesy demokratyczne (35% w stosunku do 25%).

Bardzo ciekawe wnioski płyną z analizy grup wiekowych. O ile najmłodsi badani (poniżej 24 lat) wybijają się na tle społeczeństwa ogromną obawą o zerwanie łańcuchów dostaw elektroniki (wskazuje na to aż 59% z nich), o tyle wraz z wiekiem radykalnie rośnie strach przed inwigilacją oraz paraliżem państwa. W najstarszej grupie (powyżej 55 lat) ryzyko wyłączenia infrastruktury krytycznej motywuje do działania aż 61% osób, a szpiegostwo – 58%.

Postrzeganie ryzyk jest również silnie skorelowane ze statusem społeczno-ekonomicznym i wykształceniem. Zależność jest tu prosta: im wyższe wykształcenie i zasobność portfela, tym silniejszy niepokój budzi wizja paraliżu infrastruktury oraz inwigilacji państwa. Wśród mieszkańców największych metropolii obawa przed zdalnym wyłączeniem kluczowych systemów sięga 62%, a w grupie osób o najwyższym statusie materialnym – wręcz rekordowych 90%. Z kolei osoby zmagające się z trudnościami finansowymi w dużo większym stopniu niż reszta społeczeństwa obawiają się utraty miejsc pracy i zasobów wiedzy (43%) oraz wrogich nacisków politycznych ze strony państw trzecich (57%).

Wiesław Wilk

Przewodniczący Związku Polska Chmura

Wyniki raportu potwierdzają to, o czym jako Polska Chmura mówimy od lat: problem suwerenności danych w Europie nie jest teoretyczny, lecz bardzo konkretny i systemowy. Uzależnienie od pozaeuropejskich dostawców chmurowych oznacza w praktyce ograniczoną kontrolę nad danymi, a w przypadku danych krytycznych - realne ryzyko dla ciągłości działania państwa i bezpieczeństwa obywateli.

Od lat słyszymy, że „miejsce przetwarzania danych nie ma znaczenia". To mit. W rzeczywistości lokalizacja danych jest fundamentem suwerenności cyfrowej. Jeżeli dziś w przetargu publicznym warunkiem jest, by dane były przechowywane poza granicami Polski, to w istocie sami rezygnujemy z kontroli nad tym, co kluczowe. A mówimy przecież o danych obywateli, systemach ochrony zdrowia, energetyce czy administracji publicznej.

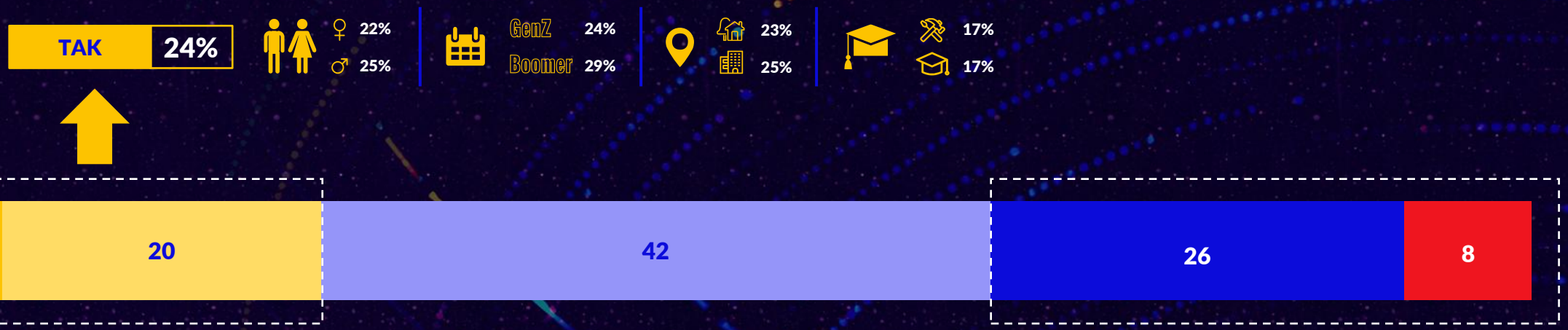
Promowany przez Komisję Europejską Cloud Sovereignty Framework jest krokiem w dobrym kierunku. Po raz pierwszy na poziomie unijnym powstało narzędzie, które pozwala w sposób ustrukturyzowany oceniać poziom suwerenności rozwiązań chmurowych, zamiast opierać się wyłącznie na deklaracjach marketingowych dostawców. Trzeba jednak jasno powiedzieć: same ramy nie odwrócą trendu, jeśli nie będą konsekwentnie stosowane i powiązane z realnymi decyzjami regulacyjnymi oraz zakupowymi państw członkowskich.

Doświadczenie pokazuje, że bez twardszych mechanizmów presja rynkowa zawsze będzie działać na korzyść globalnych gigantów, których skala i kapitał są nieporównywalne z możliwościami lokalnych operatorów. Dlatego poparcie niemal połowy badanych dla obowiązku przechowywania danych krytycznych wyłącznie u lokalnych dostawców należy traktować nie jako protekcjonizm, lecz jako wyraz rosnącej świadomości i zdrowego rozsądku. W obszarze systemów publicznych i infrastruktury krytycznej zasada ograniczonego zaufania powinna być standardem.

Dane są dziś najcenniejszym zasobem współczesnej gospodarki, szczególnie w erze AI. Jeżeli chcemy mówić o realnej niezależności państwa, musimy mieć kontrolę nad tym, gdzie informacje są przechowywane, kto je chroni i jakie prawo reguluje ich przetwarzanie. Suwerenność danych nie jest modnym hasłem, lecz jednym z fundamentów bezpieczeństwa narodowego. Z perspektywy Polskiej Chmury kluczowe jest, aby europejskie ramy suwerenności stały się podstawą realnej polityki cyfrowej, wzmacniającej lokalnych i europejskich dostawców oraz odporność państwa w coraz bardziej niepewnym świecie.

Czy jesteśmy gotowi na wyzwania suwerenności technologicznej?

Co czwarty badany (24%) wierzy, że Polska jest przygotowana. Aż 42% Polaków nie potrafi ocenić gotowości technologicznej państwa. To sygnał, że temat zaplecza technologicznego i cyberbezpieczeństwa jest dla wielu obywateli zbyt abstrakcyjny.



Pytanie jednowyborowe. Podstawa: wszyscy respondenci, N=1000 Polaków w wieku 16-75 lat
Pytanie: W jakim stopniu zgadza się Pan(i) lub nie zgadza z poniższym stwierdzeniem: Polska jest przygotowana do zapewnienia i ochrony swojej suwerenności technologicznej?

Czy jesteśmy gotowi na wyzwania suwerenności technologicznej?

Segmentacja

W ujęciu ogólnym, jedynie blisko co czwarty Polak (24%) wierzy w gotowość naszego państwa do obrony swojej niezależności w tym obszarze (z czego zaledwie 4% wyraża w tej kwestii pełne przekonanie). Wyraźnie silniejsza jest grupa sceptyków – 34% respondentów uważa, że Polska nie jest do tego przygotowana (w tym 8% twierdzi tak kategorycznie). Jednak najbardziej uderzającym wnioskiem z badania jest dominująca, bo wynosząca aż 42%, grupa osób, które wybrały odpowiedź „trudno powiedzieć". Świadczy to o tym, że dla ogromnej części społeczeństwa kwestia cyberbezpieczeństwa i zaplecza technologicznego państwa pozostaje wielką niewiadomą i tematem bardzo abstrakcyjnym.

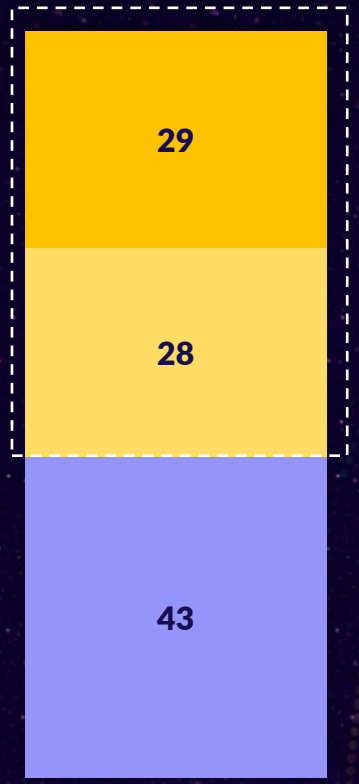
Spojrzenie na dane przez pryzmat płci ujawnia klasyczny podział na bardziej stanowczych w ocenach mężczyzn oraz ostrożniejsze w osądach kobiety. Panowie są zdecydowanie bardziej krytyczni wobec poziomu przygotowania państwa – blisko 4 na 10 z nich (39%) ocenia go negatywnie. Z kolei w grupie kobiet dominuje niepewność – aż 47% pań nie potrafi zająć jednoznacznego stanowiska, a odsetek krytyczek spada do 30%.

Najostrzejszym filtrem weryfikującym optymizm państwowy okazuje się wykształcenie. Reguła jest w tym przypadku niezwykle czytelna – im wyższe wykształcenie, tym surowsza i bardziej krytyczna ocena sytuacji. Wśród osób z dyplomem wyższej uczelni odsetek sceptyków osiąga najwyższy poziom – aż 44% z nich uważa, że Polska nie jest przygotowana do technologicznej samodzielności (optymistami jest zaledwie 17%). Z kolei w grupach z wykształceniem podstawowym i zasadniczym zawodowym brakuje przede wszystkim wiedzy lub punktu odniesienia do oceny, co manifestuje się rekordowym odsetkiem odpowiedzi „trudno powiedzieć" (odpowiednio 55% i 49%).

Podobny krytycyzm widać u osób w średnim wieku (35–44 lata), które są najbardziej pesymistyczną grupą wiekową – 42% z nich negatywnie ocenia państwowe przygotowanie. Najłagodniej w swoich ocenach wypada najstarsze pokolenie (powyżej 55. roku życia), w którym najrzadziej spotykamy się z otwartą negacją (26%), ale gdzie wciąż zdecydowanie króluje brak wyrobionej opinii (45%).

Ciekawie sytuacja prezentuje się pod kątem finansowym – największymi optymistami, deklarującymi, że państwo poradzi sobie z ochroną technologii (37% odpowiedzi twierdzących), są osoby o najwyższym statusie materialnym. Dla odmiany tzw. „klasa średnia" (osoby, którym wystarcza na podstawowe potrzeby, ale bez szaleństw) jest wybitnie niepewna (53% braku opinii) i widzi państwo w najciemniejszych barwach (tylko 11% optymistów).

Polska i Europa na pierwszym miejscu: z kim chcemy budować technologiczną niezależność?



samodzielnie, w oparciu o własne zasoby i technologie

we współpracy z krajami i instytucjami głównie z Unii Europejskiej

we współpracy z Unią Europejską oraz zaufanymi partnerami spoza Europy (takimi jak np. Stany Zjednoczone, Kanada, Australia, Korea Południowa czy Japonia)

UE / POLSKA **57%**

♀ 59%	GenZ 54%	61%	53%
♂ 55%	Boomer 48%	54%	47%

Zdecydowana większość Polaków (57%) chce budować suwerenność technologiczną wyłącznie w oparciu o zasoby krajowe (29%) lub we współpracy ograniczonej do państw i instytucji Unii Europejskiej (28%).

Wizja europejskiej i narodowej samowystarczalności technologicznej jest szczególnie silna wśród osób z wykształceniem średnim (63%) i zawodowym (62%), a także w grupie wiekowej 35–44 lata (65%).

Pytanie jednowyborowe. Podstawa: wszyscy respondenci, N=1000 Polaków w wieku 16-75 lat
Pytanie: Z kim według Pani/Pana Polska powinna rozwijać suwerenność technologiczną?

Polska i Europa na pierwszym miejscu: z kim chcemy budować technologiczną niezależność?

Segmentacja

Z analizy odpowiedzi na pytanie, z kim Polska powinna rozwijać swoją suwerenność technologiczną, płynie bardzo jasny i stanowczy komunikat – większość społeczeństwa opowiada się za ścisłym poleganiem na zasobach własnych lub europejskich. Łącząc głosy zwolenników całkowicie samodzielnej budowy niezależności (29%) z osobami stawiającymi na współpracę wyłącznie w ramach Unii Europejskiej (28%), otrzymujemy wyraźną większość na poziomie 57%. Oznacza to, że niemal sześciu na dziesięciu Polaków uważa, iż nasz kraj i kontynent mają wystarczający potencjał – lub historyczną konieczność – by w obszarze kluczowych technologii uniezależnić się od zewnętrznych potęg, rezygnując z oparcia nawet na zaufanych sojusznikach z innych kontynentów, takich jak Stany Zjednoczone czy Japonia (których wybiera 43% badanych).

Ten silny postulat budowania technologicznej „Twierdzy Europa" i opierania się na lokalnym potencjale trafia na szczególnie podatny grunt wśród osób w średnim wieku – w grupie 35–44 lata opcję krajową lub unijną wybiera łącznie aż 65% ankietowanych. Zwolennikami zamknięcia technologicznego ekosystemu w granicach Europy są również przede wszystkim osoby z wykształceniem średnim (63%) i zasadniczym zawodowym (62%), a także mieszkańcy wsi (61%), gdzie szczególnie silnie rezonuje chęć budowania suwerenności w oparciu o czysto polskie zasoby.

Z kolei otwarcie na szerokie, transatlantyckie i globalne sojusze (model mieszany) pozostaje domeną elit. Wyjście z technologiczną współpracą poza Unię Europejską, na rzecz budowania mostów m.in. z USA czy Koreą Południową, zyskuje przewagę jedynie wśród osób z wyższym wykształceniem (53% zwolenników modelu mieszanego wobec 47% dla opcji krajowej/unijnej) oraz w grupie badanych o najwyższym statusie materialnym (50% do 49%). Różnice te pokazują, że choć ogół społeczeństwa wierzy w siłę i konieczność europejskiej samowystarczalności, osoby najlepiej wykształcone i zamożne znacznie częściej uznają ją za cel niemożliwy do osiągnięcia bez wsparcia globalnych, technologicznych potęg Zachodu.

Polskie społeczeństwo skłania się ku technologicznemu uniezależnieniu w ramach kontynentu. Dominuje przekonanie o potrzebie budowy suwerenności na własnym podwórku, a szerokie, globalne sojusze postrzegane są częściej jako opcja preferowana przez osoby z wyższym statusem materialnym i naukowym.

Bartosz Łopiński

CEO Billennium, inwestor

W gospodarce cyfrowej skala nie powstaje przypadkiem - powstaje tam, gdzie kapitał, strategia i międzynarodowa ambicja spotykają się w jednym miejscu. Wyniki badania pokazują, że Polacy dobrze rozumieją tę logikę. Aż 43% respondentów wskazuje model mieszany, w którym rozwój technologii w ramach Unii Europejskiej przy jednoczesnej współpracy z zaufanymi partnerami międzynarodowymi – jako najbardziej pożądaną ścieżkę budowania konkurencyjności technologicznej.

To podejście jest realistyczne. Technologie cyfrowe rozwijają się dziś w ekosystemach, w których współpracują firmy, instytucje badawcze i administracje publiczne z różnych krajów. Kluczowe jest jednak to, aby taka współpraca prowadziła do wzmacniania europejskich kompetencji technologicznych oraz powstawania własnej własności intelektualnej w Europie. Partnerstwa międzynarodowe powinny być projektowane w taki sposób, aby europejskie firmy nie były jedynie wykonawcami usług, ale współtwórcami rozwiązań i architektury technologicznej, które mogą być rozwijane i skalowane globalnie.

W tym kontekście szczególnie istotny jest silny rynek europejski jako przestrzeń budowania pierwszych referencji technologicznych. Badanie pokazuje, że 47% Polaków popiera preferowanie europejskich produktów i usług w zamówieniach publicznych. Ten wynik należy odczytywać przede wszystkim jako oczekiwanie, że rynek publiczny będzie sprzyjał rozwojowi technologii powstających w Europie i umożliwiał im konkurowanie na równych zasadach.

Nie chodzi przy tym o protekcjonizm czy administracyjne uprzywilejowanie konkretnych firm. Najważniejsze jest tworzenie takich warunków konkurencji, które umożliwią firmom rozwijającym technologie w Europie realny dostęp do rynku i możliwość skalowania swoich rozwiązań. W praktyce oznacza to projektowanie przetargów w sposób technologicznie neutralny i skoncentrowany na funkcjonalności oraz rezultatach. Zbyt wąskie kryteria lub odwoływanie się do komercyjnych rankingów rynkowych mogą nieświadomie ograniczać konkurencję i utrudniać rozwój innowacyjnych rozwiązań powstających w Europie.

Jednocześnie badanie pokazuje rosnącą świadomość znaczenia technologii dla bezpieczeństwa gospodarczego. Aż 71% respondentów deklaruje gotowość zapłacenia wyższej ceny za technologie rozwijane w Polsce lub w Unii Europejskiej – najczęściej do około 10% więcej. W sektorach takich jak ochrona zdrowia czy zarządzanie danymi coraz wyraźniej widać, że oprócz ceny znaczenie mają także takie czynniki jak bezpieczeństwo danych, kontrola nad infrastrukturą cyfrową czy możliwość długoterminowego rozwoju systemów.

W długiej perspektywie konkurencyjność technologiczna Europy będzie zależeć od zdolności do łączenia trzech elementów: inwestycji w rozwój własnych technologii, silnego rynku wewnętrznego oraz partnerstw międzynarodowych opartych na równowadze i wzajemnej wartości. Tylko takie podejście pozwoli europejskim firmom nie tylko uczestniczyć w globalnej gospodarce technologicznej, ale także współtworzyć jej standardy i kierunki rozwoju.

Marcin Madey

Country Manager, SUSE Polska

Dane z raportu jednoznacznie wskazują, że Polacy są świadomi zagrożeń płynących z braku transparentności technologii. 29% badanych wprost wskazuje na „potencjał wystąpienia celowo ukrytych podatności na cyberataki w sprzęcie lub oprogramowaniu" jako kluczowe zagrożenie. Jest to bezpośredni dowód na brak zaufania do tzw. rozwiązań „black box" (zamkniętych), gdzie użytkownik nie ma wglądu w to, jak dokładnie działa system.

Model open source bezpośrednio neutralizuje to zagrożenie, ponieważ jego istotą jest przejrzystość i możliwość audytu kodu. W przeciwieństwie do zamkniętego oprogramowania, gdzie musimy ufać samym deklaracjom dostawcy, w modelu otwartym polskie służby i eksperci mogą samodzielnie zweryfikować każdą linię kodu pod kątem istnienia „tylnych furtek".

Zagrożenie ukrytymi podatnościami jest ściśle powiązane z dwoma innymi obawami dominującymi w raporcie: ryzykiem zdalnego wyłączenia infrastruktury przez producenta z kraju trzeciego (wskazanie 51% badanych) oraz możliwością szpiegostwa i inwigilacji przez obce służby (wskazanie 48% badanych). Open source adresuje oba zagrożenia, ponieważ oddaje kontrolę nad technologią w ręce użytkownika. Wprost zapewnia suwerenność technologiczną, która z definicji jest zdolnością do „samodzielnego kontrolowania kluczowych technologii". Ponadto umożliwia prowadzenie niezależnego audytu i wykrycie mechanizmów szpiegujących lub wyłączników („kill switch"), które mogłyby zostać ukryte w kodzie źródłowym przez dostawcę np. pod presją obcego wywiadu. I co równie ważne, open source umożliwia w razie potrzeby modyfikację i samodzielną naprawę.

Dla tych 29% Polaków obawiających się ukrytych zagrożeń, open source jest jedynym modelem technologicznym, który zamienia „zaufanie do dostawcy" na „weryfikację rozwiązania". Wdrożenie wymogu stosowania takiego oprogramowania w administracji publicznej (co obecnie popiera 39% badanych) jest więc nie tylko kwestią oszczędności, ale przede wszystkim strategicznym narzędziem eliminacji ryzyk, których społeczeństwo realnie się obawia.

Poparcie dla działań na rzecz zwiększenia autonomii Unii Europejskiej

Pytanie wielokrotnego wyboru. N=1000 Polaków w wieku 16-75 lat
Pytanie: Unia Europejska jako wspólnota państw, może podjąć różne działania do wzmocnienia jej niezależności. W jakim stopniu popiera Pan(i) lub się sprzeciwia ich wprowadzeniu?

Poparcie dla działań na rzecz zwiększenia autonomii Unii Europejskiej

Segmentacja

Badanie opinii na temat konkretnych działań i regulacji, które miałyby wzmocnić suwerenność technologiczną Unii Europejskiej, przynosi niezwykle czytelny wniosek: Polacy zdecydowanie preferują pozytywną stymulację i budowanie własnego potencjału („marchewkę") nad twardy, restrykcyjny protekcjonizm i zamykanie rynku („kij").

Na szczycie społecznego poparcia znalazły się działania ukierunkowane na rozwój i bezpieczeństwo. Największą aprobatą cieszy się postulat stworzenia programów pomocowych i dotacji na rzecz badań i rozwoju krytycznych technologii – rozwiązanie to popiera ponad połowa badanych (55%). Tuż za nim plasuje się konieczność uregulowania środowiska cyfrowego: 54% Polaków opowiada się za traktowaniem platform społecznościowych na równi z tradycyjnymi mediami (jak telewizja czy prasa), a 53% żąda wymogu posiadania europejskiego certyfikatu cyberbezpieczeństwa, zwłaszcza w sektorach krytycznych. Wysokim poparciem (47%) cieszą się również pomysły wzmocnienia koordynacji unijnej poprzez wspólne zakupy krytycznych surowców i komponentów oraz miękkie preferowanie europejskich rozwiązań w zamówieniach publicznych. Obywatele oczekują również, że wrażliwe dane (np. medyczne i podatkowe) będą bezwzględnie przechowywane i przetwarzane na terenie UE (46%).

Na przeciwległym biegunie – z wyraźnie niższym poziomem akceptacji – znalazły się mechanizmy twardego protekcjonizmu i zakazów. Polacy podchodzą ze sporym dystansem do wprowadzania nowych ceł i opłat na produkty spoza UE (tylko 38% poparcia). Najmniejszy entuzjazm budzą pomysły sztucznego ingerowania w rynek, takie jak uzależnienie dostępu do funduszy unijnych od wymogu korzystania z europejskich technologii (36%) czy wprowadzanie minimalnych, sztywnych budżetów w zamówieniach publicznych wyłącznie dla lokalnych dostawców (36%). Pokazuje to, że chcemy silnej i konkurencyjnej Europy, ale takiej, która wygrywa innowacyjnością i jakością, a nie barierami celnymi.

Analiza danych demograficznych ujawnia przy tym głębokie różnice w postrzeganiu gospodarki przez kobiety i mężczyzn. Panowie są nieporównywalnie większymi zwolennikami twardych interwencji państwowych i unijnych w rynek. Widać to doskonale na przykładzie propozycji wymogu posiadania przez zagraniczne podmioty lokalnych partnerów połączonego z transferem technologii (popiera to 53% mężczyzn i tylko 35% kobiet), nałożenia podatku cyfrowego na globalne koncerny (47% vs 35%) czy sfinansowania przeniesienia fabryk z Azji do Europy (51% vs 38%).

Kluczowym filtrem poparcia dla działań suwerennościowych pozostaje jednak wykształcenie i wiek. Im wyższe kompetencje badanych i im starsze pokolenie, tym silniejsze zrozumienie dla systemowych regulacji. Przykładowo, obowiązek posiadania certyfikatów cyberbezpieczeństwa popiera aż 65% osób po studiach wyższych (wobec 42-46% osób z wykształceniem niższym) oraz 63% osób powyżej 55. roku życia. Podobnie kształtuje się poparcie dla rygorystycznego przechowywania danych w Europie czy finansowania R&D.

Podsumowując, Polacy widzą drogę do suwerenności technologicznej przede wszystkim poprzez potężne inwestycje w unijne badania i rozwój, wymuszanie najwyższych standardów cyberbezpieczeństwa oraz ucywilizowanie globalnych gigantów cyfrowych. Zdecydowanie mniej wierzą za to w skuteczność wojen celnych czy zamykanie dostępu do unijnych pieniędzy w imię technologicznego patriotyzmu.

Krzysztof Pstrong

Dyrektor generalny, Polska Izba Komunikacji Elektronicznej (PIKE)

To jedna z najlepszych wiadomości początku 2026 roku. Polacy doskonale rozumieją, że zwiększenie nakładów na infrastrukturę i usługi telekomunikacyjne to fundament bezpieczeństwa państwa i obywateli. Jednak tym, co skutecznie hamuje rozwój sektora telekomunikacji są nadmierne obciążenia regulacyjne i fiskalne. Czas to zmienić.

Niezależny raport „Suwerenność technologiczna" przygotowany przez firmę badawczą Nielsen jednoznacznie dowodzi, że nasze społeczeństwo jest gotowe zapłacić więcej za produkty i usługi powstające na rodzimym rynku. Co ważne, raport dostarcza twardych danych, które w pełni potwierdzają nasze diagnozy i nadają im silny mandat społeczny. Potwierdza bowiem, że Polacy nie tylko rozumieją wagę suwerenności technologicznej, ale też są gotowi ponieść jej realne koszty. To kluczowy wniosek, który burzy wiele mitów narosłych wokół polskiego rynku.

Po pierwsze, aż 71% badanych akceptuje wyższą cenę produktów i usług w zamian za wspieranie rodzimych i europejskich technologii. Po drugie, niemal połowa konsumentów (45%) ma większe zaufanie do firm z polskim lub europejskim kapitałem w obszarach krytycznych, takich jak telekomunikacja.

Jako obserwator rynku cyfrowego widzę w tych liczbach nie tylko patriotyzm gospodarczy, ale przede wszystkim głęboką, dojrzałą świadomość zagrożeń płynących z nadmiernego uzależnienia od pozaeuropejskich gigantów.

Kluczowym wnioskiem z tej analizy jest fakt, że ponad połowa obywateli uznaje niezależność cyfrową za fundament bezpieczeństwa państwa. Fakt, że niemal połowa z nas darzy większym zaufaniem rozwiązania z rodzimym lub unijnym kapitałem, stanowi kluczowy argument dla lokalnych innowatorów i decydentów. Konsumenci dostrzegają bowiem, że suwerenność to nie tylko abstrakcyjne hasło, ale realna ochrona przed dezinformacją płynącą z platform społecznościowych oraz gwarancja ciągłości dostaw półprzewodników czy energii.

Co to oznacza w praktyce? Że dotychczasowa, nieproporcjonalna determinacja regulatora w utrzymywaniu presji na niskie ceny stoi w jawnej sprzeczności z oczekiwaniami społecznymi i strategicznym interesem państwa.

Marcin Madey

Country Manager, SUSE Polska

Z raportu wynika, że główną barierą we wdrażaniu otwartego oprogramowania w polskiej administracji nie jest technologia ani otwarty sprzeciw, lecz ogromna luka edukacyjna i brak świadomości. To bariera mentalna: „Nie wiem, więc nie popieram" - 47% badanych nie ma zdania („trudno powiedzieć") w kwestii wymogu stosowania open source w urzędach, a sprzeciw deklaruje łącznie tylko 15%. To nie mit o „braku bezpieczeństwa" jest głównym problemem, ale brak zrozumienia definicji open source. Połowa społeczeństwa nie wie, że „przejrzystość i możliwość audytu kodu" to synonimy cyfrowego bezpieczeństwa, którego tak bardzo oczekują. Problemem ukrytych podatności martwi się aż 29% Polaków.

Poparcie dla open source jest nierównomiernie rozłożone, co wskazuje, do kogo należy kierować działania edukacyjne. Przykładowo, kobiety rzadziej popierają korzystanie z open source (36%) niż mężczyźni (42%), ale wynika to z gigantycznej niepewności – aż 52% kobiet wybrało odpowiedź „trudno powiedzieć" (wobec 41% mężczyzn). Spore problemy ze zrozumieniem tematu mają osoby z wykształceniem zasadniczym zawodowym – aż 57% z nich nie ma zdania. Z kolei osoby z wykształceniem wyższym częściej deklarują zdecydowane poparcie (15%). W największych miastach (>500 tys.) „zdecydowane poparcie" jest najwyższe (17%), co sugeruje, że tam świadomość technologiczna jest największa.

Jak więc przełamywać te bariery? Żeby zwiększyć adopcję open source, narracja musi ulec zmianie. Po pierwsze edukacja - kluczem jest prosta komunikacja łącząca open source z suwerennością. Polacy chcą niezależności (56% uważa ją za ważną), ale nie widzą jeszcze związku między „otwartym kodem" a „bezpieczeństwem narodowym". Trzeba podnosić też argument ekonomiczny i bezpieczeństwa podkreślając, że open source to nie tylko „darmowa licencja", ale przede wszystkim eliminacja „tylnych furtek" (backdoors) i uniezależnienie od zagranicznych dostawców - co bezpośrednio odpowiada na lęk przed zdalnym wyłączeniem infrastruktury (obawa się tego 51% Polaków).

Podsumowując, barierą dla pozytywnego podejścia do stosowania open source nie jest niechęć, lecz niewiedza. A potencjał do wzrostu poparcia jest ogromny, jeśli przekonamy grupę „niezdecydowanych", że otwarty kod to fundament cyfrowego bezpieczeństwa państwa.

PRZEGLĄD DZIAŁAŃ INNYCH PAŃSTW Z ZAKRESU SUWERENNOŚCI TECHNOLOGICZNEJ

Brazylia

Kluczowe filary – „względna autonomia", cyfrowe samostanowienie i hybrydowe podejście - dla Brazylii, największej gospodarki Ameryki Łacińskiej, suwerenność technologiczna nie oznacza dążenia do pełnej izolacji i samowystarczalności (autarkii), lecz budowę „względnej autonomii" i strategicznej sprawczości napędzającej narodowy rozwój. Podejście to jest w pełni hybrydowe: łączy rynkowy dynamizm gospodarki USA, interwencjonizm i reindustrializację państwową oraz rygorystyczne ukierunkowanie na ochronę praw jednostki zapożyczone z Unii Europejskiej. Model ten opiera się na kluczowych filarach: bezpośredniej kontroli nad publiczną infrastrukturą cyfrową (aby wyeliminować prywatnych pośredników) , twardej polityce przemysłowej i reindustrializacji z budżetem rzędu 300 mld BRL, agresywnym wykorzystywaniu regulacji prawnych jako instrumentu siły oraz aktywnym przywództwie i dyplomacji w ramach Globalnego Południa.

Wizja suwerenności technologicznej – twarde prawo i ochrona kultury Brazylijska wizja cyfrowej suwerenności jest głęboko zakorzeniona w konstytucjonalizmie i aktywnej roli państwa. Państwo nie waha się bezwzględnie wykorzystywać swoich instytucji, w tym Sądu Najwyższego (STF), do zmuszania globalnych korporacji do respektowania lokalnego prawa – czego bezprecedensowym dowodem na skalę świata była drastyczna blokada serwisu X (dawniej Twitter) za szerzenie dezinformacji i brak przedstawicielstwa prawnego. Równolegle suwerenność w dobie AI jest postrzegana przez pryzmat ochrony dziedzictwa: Brazylia ogromnie inwestuje we własne modele językowe trenowane na portugalskich danych (projekt „SoberanIA"), aby uchronić się przed postępującą „kolonizacją algorytmiczną" przez systemy amerykańskie. Kraj aspiruje do miana "protagonisty innowacji", który ustala zasady gry, a nie tylko konsumuje zachodnie technologie.

Koordynacja polityk i wdrożenia (MCTI, MGI i CIT Digital) – architektura decyzyjna opiera się na kilku potężnych instytucjach, choć system ten wciąż boryka się z pewną resortową fragmentacją. Strategiczne kierunki polityki naukowej i rozwoju sztucznej inteligencji wyznacza Ministerstwo Nauki, Technologii i Innowacji (MCTI) , podczas gdy cyfryzacją administracji operacyjnie zarządza Ministerstwo Zarządzania i Innowacji w Usługach Publicznych (MGI) wspólnie z silnymi, państwowymi spółkami informatycznymi – Serpro i Dataprev. Przełomem dla cyfrowej niezależności było nadanie Krajowemu Organowi Ochrony Danych (ANPD) statusu w pełni niezależnej agencji o gigantycznych uprawnieniach regulacyjnych. Z kolei nad strategicznym cyberbezpieczeństwem czuwa kontrolowany przez wojsko Gabinet Bezpieczeństwa Instytucjonalnego (GSI).

Finansowanie i strategie, ulgi – PBIA i program Brazil Semicon - Brazylia zbudowała najgęstszą sieć publicznego finansowania innowacji w całej Ameryce Łacińskiej. Fundamentem jest nowa strategia polityki przemysłowej „Nova Indústria Brasil" (NIB) dysponująca budżetem ponad 300 mld BRL (ok. 60 mld USD). Główne ramię finansowe stanowią bank BNDES oraz agencja FINEP, dostarczające miliardy na transformację. Kluczowym przedsięwzięciem bezpośrednio wspierającym suwerenność cyfrową jest Narodowy Plan Sztucznej Inteligencji (PBIA 2024–2028), na który rząd przeznaczył aż 23 mld BRL. Środki te zasilą m.in. modernizację potężnego narodowego superkomputera Santos Dumont. Ekosystem ten katalizuje potężny kapitał prywatny, w tym rynek funduszy venture capital, który w 2024 r. zasilił lokalne startupy kwotą blisko 5 mld USD. dodatkowo latem 2024 roku zatwierdzono program „Brazil Semicon", wprowadzający masowe ulgi podatkowe i zachęty finansowe dla wzmocnienia krajowej produkcji układów scalonych.

...

...

Preferencje dla lokalnych firm i zamówienia publiczne (PPI) i ulgi podatkowe – Brazylia świadomie wykorzystuje zamówienia publiczne jako narzędzie stymulacji krajowych innowacji (ang. Public Procurement of Innovation). Brazylia stosuje zaawansowany system miękkiego protekcjonizmu i wsparcia lokalnych graczy. W zamówieniach publicznych urzędy mogą legalnie stosować marżę preferencji wynoszącą do 25 proc., co pozwala wybierać droższe, ale tworzone w kraju produkty i oprogramowanie. Ochronę rynku gwarantują potężne narzędzia fiskalne.

- **Lei do Bem -** stawa oferująca firmom tzw. super odliczenie – mogą one odpisać od podatku dochodowego aż 160–180% kosztów poniesionych na R&D w kraju.
- **Program REDATA (2025)** - radykalny reżim podatkowy znoszący m.in. cła na sprzęt dla centrów danych, ale uwarunkowany twardo: podmioty muszą używać 100% czystej energii, reinwestować 2% capexu w lokalne B+R oraz rezerwować 10% mocy obliczeniowej dla rynku brazylijskiego.
- **Programy PADIS i Lei de Informática** - gwarantujące masowe zniżki celne i podatkowe (wyceniane na ponad 2,5 mld USD) dla krajowych producentów elektroniki i układów scalonych. Dodatkowo prawo wymusza na firmach z sektorów regulowanych (np. energetyka, telekomunikacja) obligatoryjne przeznaczanie części swoich przychodów na badania i rozwój na terytorium Brazylii.

Współpraca z rynkiem – skrajny pragmatyzm i koncepcja „Nuvem Soberana” – podejście rządu do zagranicznego big techu najlepiej widać na przykładzie inicjatywy Suwerennej Chmury (Nuvem de Governo / Nuvem Soberana) z 2024 roku. Instytucje państwowe zostały zmuszone do przenoszenia wrażliwych danych (podatkowych, rejestrów obywatelskich) do chmury kontrolowanej wyłącznie przez państwowe spółki Serpro i Dataprev. Brazylia nie buduje jej jednak od zera w izolacji bo zawiera technologiczne partnerstwa z takimi gigantami jak AWS, Google, Oracle, Huawei czy Microsoft. Ich zaawansowany sprzęt i systemy instalowane są jednak fizycznie we wnętrzu chronionych, państwowych centrów danych, a całkowity nadzór operacyjny i zarządzanie kluczami szyfrującymi pozostaje bezwzględnie w rękach brazylijskich urzędników, zgodnie z twardym prawem ochrony danych (LGPD). Jednocześnie Brazylia unikalnie zarządza innowacjami: państwowa agencja EMBRAPII dofinansowuje 1/3 kosztów ryzykownych badań pod warunkiem, że kapitał prywatny i uczelnie również dorzucą swoje części, a rozwojem samego internetu kieruje ustrukturyzowany komitet CGI.br, gdzie rząd, biznes i naukowcy mają równy głos.

Dyplomacja i eksport czyli przywództwo Globalnego Południa - kraj wykorzystuje swoje sukcesy technologiczne jako filar nowej polityki zagranicznej. Podczas prezydencji w G20 oraz w ramach współpracy państw BRICS, Brazylia agresywnie promuje model wielostronnego, zrównoważonego zarządzania siecią i AI (często kontrując interesy amerykańskie czy chińskie). Ogromnym sukcesem dyplomatycznym i eksportowym (*soft power*) jest dzielenie się z państwami afrykańskimi i latynoamerykańskimi bezkonkurencyjnymi technologiami brazylijskimi – w szczególności systemem natychmiastowych płatności PIX oraz wiedzą z zakresu technologii rolniczych (Agritech) tworzonych przez instytut EMBRAPA. Postawa ta – zwłaszcza w konfrontacji z platformą X – udowodniła globalnie, że państwo potrafi narzucić własne reguły najsilniejszym graczom na rynku.

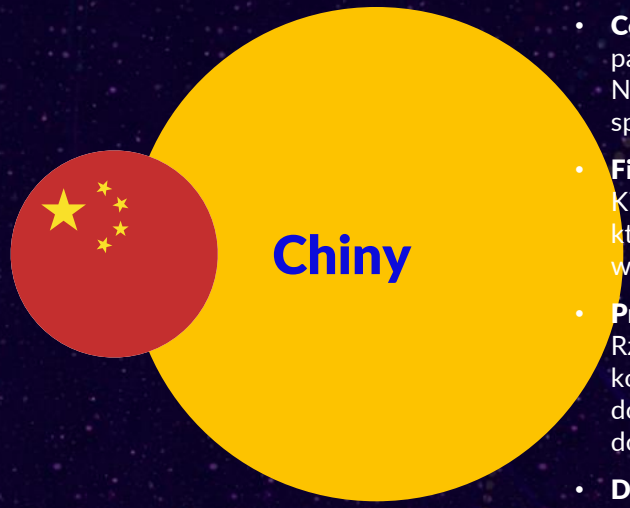
...

Brazylia

...

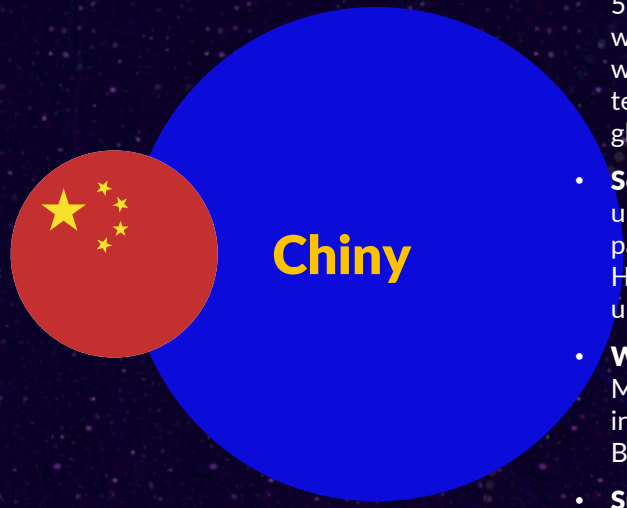
Kluczowe technologie i sektory – AI, open source i odbudowa sektora półprzewodników (CEITEC) – strategia technologiczna Brazylii opiera się na kilku filarach sprzętowo-programowych:

- **Sztuczna Inteligencja (Soberana AI)** - budowa rodzimych dużych modeli językowych (LLM), regulacja sztucznej inteligencji zorientowana na prawa człowieka oraz wykorzystywanie algorytmów na szeroką skalę do poprawy polityk opieki społecznej. Wdrożenia koncentrują się na realnych zastosowaniach AI w obszarach zdrowia, edukacji i usług publicznych.
- **Półprzewodniki** - aby uniezależnić się od szantażu w łańcuchach dostaw, państwo podjęło głośną decyzję o zrewitalizowaniu i ponownym otwarciu zlikwidowanej w 2020 r. państwowej spółki CEITEC (posiadającej jedyną na kontynencie południowoamerykańskim fabrykę klasy *front-end*). Ośrodek ten skupia się obecnie na produkcji układów zasilania oraz m.in. chipów RFID niezbędnych w sektorze rolniczym (np. do elektronicznego monitorowania narodowego pogłowia bydła). Uruchomiło również ustawą Brasil Semicon, stymulując miliardowe inwestycje w projektowanie i enkapsulację układów.
- **Open source** - zabezpieczeniem przed zjawiskiem *vendor lock-in* jest w Brazylii mocno zakorzeniony nurt rozwoju oprogramowania open source. Kraj ten ma wieloletnie tradycje używania darmowych narzędzi (od systemów Linux na urzędniczych biurkach po otwarte biblioteki kodu), co dzisiaj silnie łączy się z infrastrukturą *Nuvem Soberana*.
- **Agritech** - Brazylia jest technologicznym hegemonem w rolnictwie precyzyjnym (zakładając dojście do 95% produkcji maszyn w kraju).
- **Fintech (DPI)** - system PIX stał się absolutnym wzorcem publicznej infrastruktury cyfrowej (DPI), z ponad 150 mln użytkowników i rynkiem wartym biliony reali, minimalizując zależność od poza brazylijskich operatorów płatniczych.



- **Kluczowe filary to samowystarczalność (ang. *self-reliance*) i tzw. podwójny obieg** - dla Pekinu suwerenność technologiczna nie jest jedynie kwestią gospodarki, ale fundamentalnym filarem bezpieczeństwa narodowego i przetrwania w obliczu rywalizacji z USA. Państwo odeszło od modelu opartego na eksporcie tanich towarów na rzecz strategii podwójnego obiegu (ang. Dual Circulation) oraz inicjatywy „Made in China 2025". Cel jest jasny – to całkowite uniezależnienie się od zachodnich technologii, osiągnięcie dominacji w tzw. nowych obszarach produkcji (AI, zielone technologie, technologie kwantowe, technologie kosmiczne i biotechnologie) i zmuszenie reszty świata do polegania na chińskich łańcuchach dostaw.
- **Centralna koordynacja (CAC, MIIT i NDRC)** - chińska polityka cyfrowa jest silnie scentralizowana i zarządzana przez potężne organy państwowe. Ministerstwo Przemysłu i Technologii Informacyjnych (MIIT) steruje polityką przemysłową i rozwojem infrastruktury (jak 5G), Narodowa Komisja Rozwoju i Reform (NDRC) rozdziela gigantyczne środki finansowe, a Administracja Cyberprzestrzeni Chin (CAC) sprawuje totalitarną kontrolę nad internetem, danymi obywateli i algorytmami korporacji.
- **Finansowanie innowacji (ang. Government Guidance Funds)** - model finansowania w Chinach opiera się na tzw. Rządowych Funduszach Kierunkowych. Są to tysiące funduszy zasilanych państwowym i samorządowym kapitałem o łącznej wartości licznej w bilionach juanów, które działają jak gigantyczne fundusze VC. Państwo przekierowało kapitał z sektora internetu konsumenckiego (np. gry, e-commerce) w stronę tzw. hard-tech (produkcja zaawansowana, robotyka, baterie solid-state, lotnictwo).
- **Program "Małych Gigantów" (ang. Little Giants)** - odpowiednik koreańskiego wsparcia dla MŚP, ale nastawiony ściśle na przemysł. Rząd centralny identyfikuje i certyfikuje tysiące wysoce wyspecjalizowanych, niszowych firm technologicznych, które tworzą krytyczne komponenty (np. mikrozawory, lasery, specjalistyczne smary). Otrzymują one potężne ulgi podatkowe, dotacje i preferencyjny dostęp do giełdy w Pekinie, aby uszczelnić luki w chińskich łańcuchach dostaw i uniezależnić produkcję od Zachodu. Skala: 100 tys. firm (2025), dotacje >1 bln CNY, ulgi 30% B+R.
- **Doktryna Xinchuang (Zikong) i Dyrektywa 79** - Chiny realizują bezwzględną politykę usuwania zagranicznych technologii z krajowej infrastruktury, znaną pod hasłem "Bezpieczne i Kontrolowane" (Zikong) oraz w ramach inicjatywy Xinchuang. Słynny, niejawny „Dokument 79" nakazał wszystkim państwowym przedsiębiorstwom (SOE) oraz instytucjom rządowym całkowitą wymianę zagranicznego oprogramowania (np. Windows, Oracle) i sprzętu (np. serwery HP czy Dell) na krajowe odpowiedniki do 2027 roku. Stanowi to gigantyczną, odgórnie sterowaną kroplówkę finansową dla rodzimych dostawców IT.

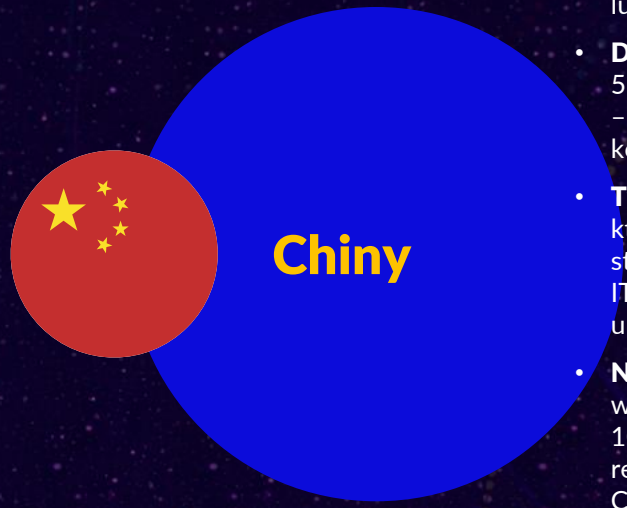
...



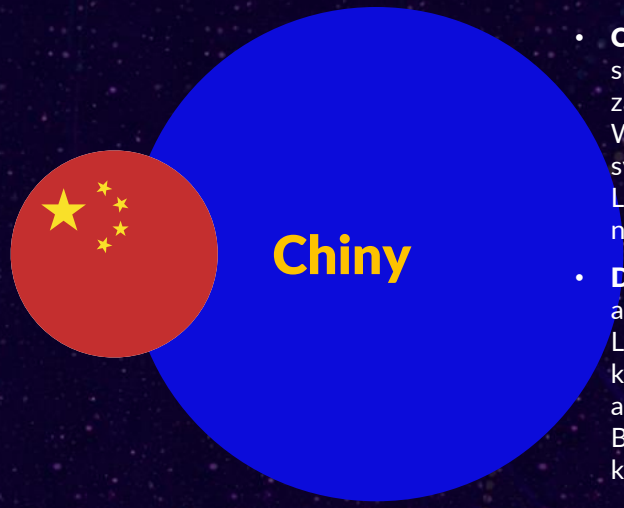
...

- **Cyfrowy Jedwabny Szlak (Digital Silk Road) i kredyty eksportowe** - to technologiczne ramię potężnej Inicjatywy Pasa i Szlaku, służące agresywnej ekspansji chińskiej suwerenności cyfrowej na zewnątrz. Pekin wykorzystuje potęgę swoich państwowych instytucji finansowych (jak Exim Bank of China), oferując państwom Globalnego Południa (w Afryce, Azji czy Ameryce Łacińskiej) gigantyczne kredyty eksportowe, których łączną wartość szacuje się na około 200 miliardów USD. Mechanizm ten jest genialny w swojej prostocie: rządy krajów rozwijających się otrzymują bardzo tanie finansowanie na budowę nowoczesnej infrastruktury (światłowodów podmorskich, sieci 5G, systemów monitoringu "smart city" czy centrów danych), ale pod twardym warunkiem, że wykonawcami i dostawcami sprzętu będą wyłącznie chińskie firmy (takie jak Huawei, ZTE, Hikvision czy Alibaba). W ten sposób państwo chińskie za jednym zamachem dotuje własny Big Tech, rozwiązuje problem nadpodaży na rynku wewnętrznym, uzależnia technologicznie dziesiątki państw od swoich technologii i – co najważniejsze dla suwerenności – narzuca światu chińskie standardy cyfrowe oraz zyskuje strategiczny dostęp do globalnych przepływów danych.
- **Sektor półprzewodników i „big fund”** - w odpowiedzi na amerykańskie sankcje, odcinające Chiny od nowoczesnych procesorów, Pekin uruchomił Narodowy Fundusz Inwestycyjny Przemysłu Układów Scalonych (znany jako "big fund"). W trzech dotychczasowych fazach państwo wpompowało w niego dziesiątki miliardów dolarów. Środki te trafiają bezpośrednio do takich czempionów jak SMIC czy Hua Hong, aby masowo subsydiować budowę nowych fabryk (tzw. dojrzałych technologii/legacy chips) i zmonopolizować globalny rynek układów scalonych starszej generacji, używanych m.in. w motoryzacji i AGD. Cel to 70% samowystarczalności w legacy chips do 2027.
- **Własny big tech i wielka zapora sieciowa (ang. Great Firewall)** - Chiny od lat blokują dostęp do zachodnich platform (Google, Meta/Facebook, X/Twitter, Amazon), budując własny, odizolowany ekosystem cyfrowy. Ten drastyczny protekcjonizm pozwolił na inkubację i gigantyczny wzrost narodowych czempionów, takich jak Tencent (twórca super-aplikacji WeChat), Alibaba, Baidu czy ByteDance (właściciel TikToka/Douyin). Firmy te oferują państwu pełen wgląd w dane i stanowią cyfrowy kręgosłup kraju.
- **Suwerenny open source i architektura RISC-V** - Chiny zdały sobie sprawę, że uzależnienie od amerykańskiego GitHuba to ryzyko. Dlatego rząd powołał i wspiera własne repozytorium kodu – Gitee. Dodatkowo państwowe podmioty masowo inwestują w rozwój otwarto źródłowej architektury procesorów RISC-V, aby obejść amerykańskie i brytyjskie licencje (x86 i ARM). Z kolei Huawei, po odcięciu od Androida, przy mocnym wsparciu państwa rozwija systemy operacyjne OpenHarmony (dla urządzeń mobilnych i IoT) oraz openEuler (dla serwerów), by stworzyć w pełni niezależny, chiński stos technologiczny. OpenHarmony (od 2020 r., pod OpenAtom Foundation) osiągnął w 2025 r. wersję 5.0 (API 12), z HarmonyOS NEXT całkowicie wolnym od Androida.

...

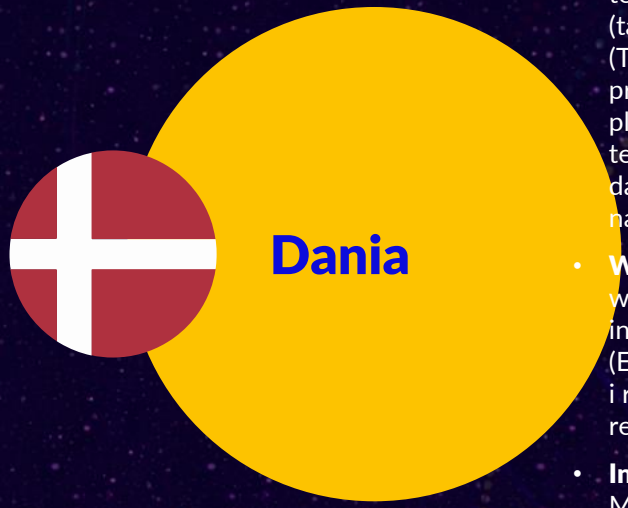


- **Suwerenność danych (PIPL i DSL)** - Chiny wprowadziły jedne z najbardziej surowych reżimów danych na świecie w 2021 roku. To Ustawa o Ochronie Danych Osobowych (PIPL) roku oraz Ustawa o Bezpieczeństwie Danych (DSL) . Prawo to kategorycznie zmusza globalne firmy (jak Apple czy Tesla) do budowania centrów danych na terenie Chin (np. w prowincji Guizhou) i przechowywania tam danych chińskich użytkowników. Wywiezienie jakichkolwiek ważnych danych za granicę wymaga zgody państwa i przejścia rygorystycznego audytu bezpieczeństwa, co daje władzom pełną kontrolę nad cyfrowym śladem populacji i gospodarki. Naruszenia grożą karami do 50 mln CNY lub 5% obrotu globalnego.
- **Dominacja w infrastrukturze 5G i sieciach światłowodowych (Huawei i ZTE)** - Chiny zbudowały największą na świecie, autonomiczną sieć 5G standalone, posiadając miliony stacji bazowych. Państwo mocno subsydiuje i chroni swoich producentów sprzętu telekomunikacyjnego – Huawei i ZTE. Dzięki państwowym liniom kredytowym firmy te mogą oferować swoje usługi na świecie znacznie poniżej kosztów konkurencji (np. z Europy), co jest elementem szerszej ekspansji geopolitycznej znanej jako „Cyfrowy Jedwabny Szlak”.
- **Tworzenie własnych standardów globalnych (China Standards 2035)** - dla Chin najwyższym stopniem suwerenności jest sytuacja, w której to inni muszą dostosować się do ich reguł. Zgodnie z planem "*China Standards 2035*", Pekin agresywnie promuje swoje własne standardy techniczne (np. w dziedzinie smart city, komunikacji kwantowej, kamer przemysłowych) w międzynarodowych organizacjach (np. ITU, ISO). Chiny wymuszają również na zagranicznych dostawcach stosowanie chińskich algorytmów kryptograficznych (np. serii SM) w urządzeniach sprzedawanych na rynku wewnętrznym.
- **Narodowy Plan AI 2030 i fuzja cywilno-wojskowa** - Pekin traktuje sztuczną inteligencję jako najważniejszą broń w technologicznym wyścigu zbrojeń. W ramach planu "New Generation Artificial Intelligence Development Plan" państwo przeznaczyło na start budżet rzędu 100 miliardów CNY (ok. 15 mld USD) na rozwój AI, z twardym celem stania się bezwzględnym światowym liderem do 2030 roku. Łączne realne nakłady (z prowincjami/firmami) przekraczają 1 bln CNY rocznie (2025: 3,3 bln CNY R&D ogółem, z AI jako priorytetem). Chiny masowo dotują i rozwijają potężne, rodzime modele fundamentowe (takie jak WuDao czy Baichuan), które mają konkurować z rozwiązaniami z Doliny Krzemowej. Co kluczowe, rozwój ten jest ściśle powiązany z doktryną fuzji cywilno-wojskowej – najnowocześniejsze cywilne algorytmy AI są natychmiast integrowane z systemami Chińskiej Armii Ludowo-Wyzwoleńczej (PLA) do tworzenia np. autonomicznych systemów uzbrojenia i analizy wywiadowczej.



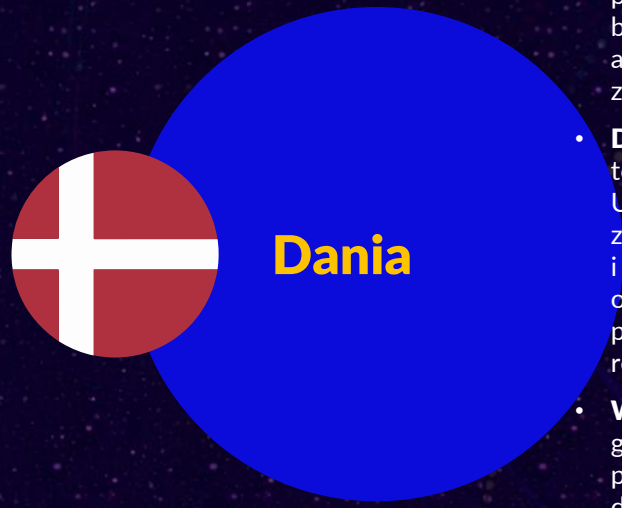
...

- **Cybersecurity Law i czystka zachodnich procesorów (MLPS 2.0)** - chińska cyber-suwerenność oznacza fizyczne wykluczenie zachodniego sprzętu z infrastruktury państwa. Opierając się na Ustawie o Bezpieczeństwie Cybernetycznym z 2017 r. oraz rygorystycznych, zaktualizowanych w 2024 roku standardach ochrony infrastruktury (MLPS 2.0), rząd stworzył czarne listy niebezpiecznych technologii. W efekcie, zagraniczne procesory (m.in. układy firm Intel czy AMD o architekturze powyżej 16nm) są metodycznie usuwane z krajowych systemów telekomunikacyjnych, bankowości oraz wojska. W ich miejsce masowo wdraża się chińskie odpowiedniki (takie jak procesory Loongson czy Phytium). Ta rządowa, przymusowa wymiana sprzętu napędza potężny, całkowicie wewnętrzny rynek szacowany na 1 bilion CNY rocznie.
- **Dominacja w technologiach kwantowych i kosmicznych (Beidou)** - Chiny inwestują bezprecedensowe środki w „technologie jutra", aby upewnić się, że to one będą ustalać nowe zasady gry. Państwo zainwestowało ponad 100 miliardów CNY w budowę Narodowego Laboratorium Nauk Kwantowych (National Quantum Lab), dążąc do wygrania wyścigu o komputery kwantowe i niemożliwą do złamania komunikację. Równolegle państwo osiągnęło całkowitą suwerenność informacyjną w kosmosie – zrezygnowało z polegania na amerykańskim systemie GPS, budując od zera, wdrażając i globalnie promując własny, w pełni niezależny system nawigacji satelitarnej Beidou. Sukcesy te dopełnia ambitny państwowy program kosmiczny (w tym zaawansowane misje księżycowe, takie jak Chang'e-6), który udowadnia pełną niezależność Chin od zachodniej myśli inżynieryjnej.

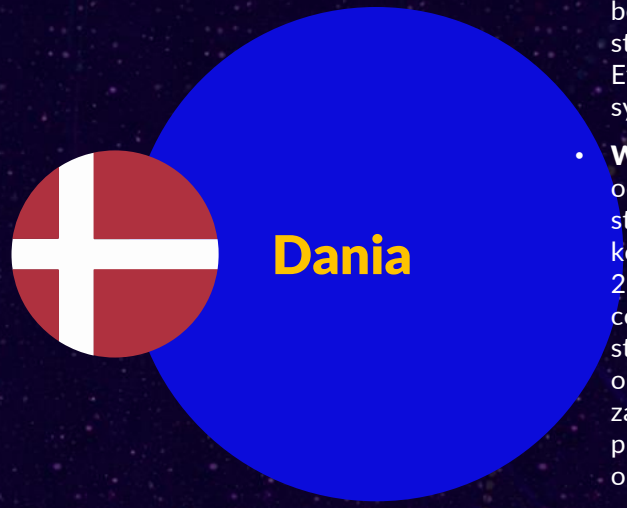


- **Kluczowe filary: oddolna niezależność operacyjna, migracje rozwiązań z big tech, open source i TechPlomacy** – Dania buduje swoją suwerenność technologiczną (digital suveræ nitet) w sposób pragmatyczny i odmienny od globalnych mocarstw, unikając izolacji czy tworzenia odrębnego narodowego internetu (na wzór Rosji czy Chin) na rzecz operacyjnej, klasycznej samokontroli operacyjnej nad państwową infrastrukturą IT i danymi we współpracy z przedsiębiorcami. Strategia ta, ugruntowana m.in. w Narodowej Strategii Cyfryzacji 2022 (obejmującej 61 inicjatyw), opiera się na kategorycznym unikaniu uzależnienia od pojedynczych, zagranicznych dostawców (ang. *vendor lock-in*) poprzez odgórne zasady architektoniczne promujące otwarte standardy oraz oddolne inicjatywy współdzielonego oprogramowania open source, co świetnie widać na przykładzie działań wspólnoty OS2. Zamiast kategorycznie odcinać się od globalnych technologii, Dania stawia na silne e-państwo, cyberbezpieczeństwo i interoperacyjność kontrolowanych przez państwo węzłów cyfrowych (takich jak platforma GovCloud czy systemy eID). Równocześnie Kopenhaga wdraża unikalną na skalę światową dyplomację technologiczną (TechPlomacy), wpływając bezpośrednio na zarządy gigantów technologicznych, oraz rygorystycznie koduje duńskie wartości etyczne w prawie, chroniąc obywateli i ich podmiotowość przed dominacją platform (m.in. poprzez nowe prawo dotyczące deepfake'ów czy planowany zakaz mediów społecznościowych dla dzieci). Fundamentem duńskiej suwerenności jest wizja „Digital Welfare State", w której technologia wzmacnia państwo opiekuńcze, zwiększa odporność instytucji publicznych i gwarantuje obywatelom pełną kontrolę nad danymi. W przeciwieństwie do Chin czy Korei Południowej Dania nie buduje zamkniętego ekosystemu technologicznego, lecz stawia na otwarte standardy i mocną współpracę europejską.
- **Wizja suwerennej Europy i współpraca regionalna** – Dania postrzega suwerenność technologiczną nie jako narodową izolację, lecz jako wspólny projekt realizowany w ścisłej współpracy z państwami nordyckimi i całą Unią Europejską. Zamiast budować zamknięty „narodowy internet", Kopenhaga angażuje się w tworzenie interoperacyjnej infrastruktury unijnej, takiej jak europejska tożsamość cyfrowa (EUDI Wallet) czy wspólne standardy danych. Jako jedno z najbardziej ucyfrowionych społeczeństw w Europie i lider odporności i rezyliencji (2025 FM Resilience Index), Dania wykorzystuje swoje doświadczenie, by stać się liderem w kształtowaniu europejskich regulacji (np. AI Act, NIS2, RODO) w oparciu o prawa człowieka.
- **Instytucje i koordynacja polityk cyfrowych** – głównym ośrodkiem decyzyjnym i architektem państwowych systemów IT jest podlegająca Ministerstwu Finansów Agencja ds. Cyfryzacji (*Digitaliseringsstyrelsen – Digst*). Odpowiada ona za rozwój infrastruktury cyfrowej, zarządzanie systemami e-tożsamości, projektowanie wspólnych standardów technologicznych oraz ścisłą koordynację polityki (w tym *Joint Government Digital Strategy*) między rządem centralnym, regionami i gminami, co tworzy silnie scentralizowany model zarządzania. Działania Agencji wspiera Centrum Cyberbezpieczeństwa (CFCS), egzekwujące wymogi unijnej dyrektywy NIS2 i monitorujące zagrożenia w zakresie inwigilacji i szpiegostwa przemysłowego, oraz powołana w 2024 roku Etyczna Rada ds. AI (*Etisk Råd for AI*), nadzorująca odpowiedzialne wdrażanie technologii. Unikalnym na skalę światową przedłużeniem tej państwowej koordynacji jest dyplomacja technologiczna (TechPlomacy) i urząd Ambasadora Technologicznego, który prowadzi bezpośrednie, twarde negocjacje z zarządami amerykańskich big techów w Dolinie Krzemowej, traktując je jak podmioty o wpływach równych państwom.

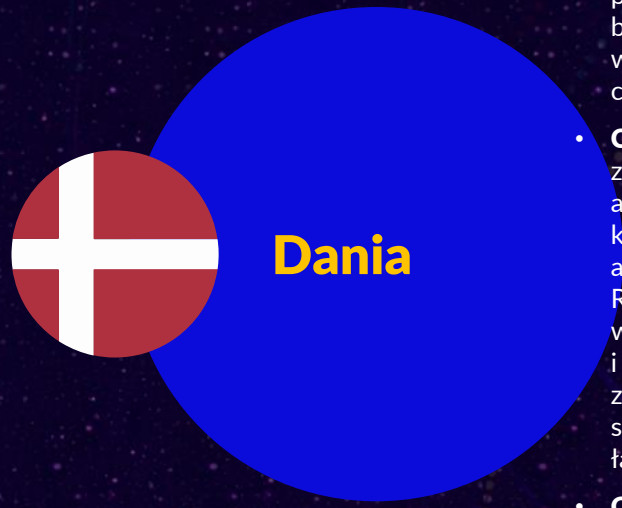
...



- **Strategie i fundusze** – duńska polityka cyfrowa opiera się na wieloletnich programach, z których fundament stanowi Narodowa Strategia Cyfryzacji 2022 , obejmująca 61 inicjatyw (m.in. cyberbezpieczeństwo, zieloną transformację i budowę etycznej bazy cyfrowej) ze wsparciem inwestycyjnym rzędu 800 mln DKK. Jej kluczowym elementem jest architektoniczna zasada 2.3 („Unikaj zależności od dostawców i technologii z unikalnym IP"), która, wzmocniona oficjalnymi wytycznymi z 2024 roku, nakazuje państwowej administracji preferowanie rozwiązań open source w celu zachowania pełnej kontroli nad kodem źródłowym i danymi. Działania te rozwija nowa, wspólna strategia rządu i samorządów (Joint Government Digital Strategy 2026-2029), kładąca nacisk na spójne e-usługi, cyfrowe pełnomocnictwa oraz suwerenność cyfrową. Integralną częścią tych planów jest państwowa strategia sztucznej inteligencji, zasilana budżetem 740 mln DKK na lata 2024-2027 (oraz 18 mln DKK na projekty badawcze dla MŚP), która zakłada stworzenie administracyjnego asystenta AI, piaskownicy regulacyjnej oraz duńskich, otwarto źródłowych modeli językowych, aby aktywnie redukować technologiczną zależność państwa od zagranicznych modeli, takich jak OpenAI ChatGPT czy Microsoft Co-Pilot.
- **Dyplomacja cyfrowa i TechPlomacy („miękka suwerenność")** – Dania jako pierwszy kraj na świecie, już w 2017 roku, oficjalnie wpisała technologię do swojej strategii polityki zagranicznej, powołując unikalny urząd Ambasadora Technologicznego z globalnym mandatem. Urzędując m.in. w Dolinie Krzemowej, pełni on rolę swoistej „ambasady wobec big techów", traktując globalne korporacje technologiczne z powagą równą państwom. Celem tej innowacyjnej strategii jest zastąpienie twardego protekcjonizmu bezpośrednimi negocjacjami i wpływanie na zarządy gigantów w duchu poszanowania praw człowieka, wczesne ostrzeganie własnego rządu o nowych trendach oraz transfer eksperckiej wiedzy do polityk krajowych. Zamiast biernie reagować na narzucane z zewnątrz standardy, Dania chce siedzieć przy stole, gdzie one powstają. Pozwala to Danii nie tylko chronić własne interesy, ale też aktywnie współkształtować kluczowe unijne regulacje cyfrowe, takie jak DSA, DMA czy AI Act.
- **Wdrożenie suwerenności technologicznej pozwala redukować koszty mimo wyższych początkowych nakładów finansowych** – głównym motywatorem duńskiego zwrotu technologicznego są drastycznie rosnące koszty licencji komercyjnych, co jaskrawo widać na przykładzie Kopenhagi, gdzie wydatki na usługi Microsoftu wzrosły aż o 72 proc. w ciągu zaledwie pięciu lat (z 313 mln DKK w 2018 r. do 538 mln DKK w 2023 r.). Chociaż w kraju występuje swoisty paradoks – państwo w 2025 r. równolegle podpisało z Microsoftem rekordowy, pięcioletni kontrakt na 4,2 mld DKK oraz umowy na globalne chmury (m.in. AWS, Google) warte 5,7 mld DKK – to długofalowa, pragmatyczna kalkulacja zdecydowanie faworyzuje budowę własnych alternatyw. Potencjalne oszczędności są bezprecedensowe - koszt otwarto źródłowej platformy AI wynosi zaledwie 25 DKK na pracownika rocznie, podczas gdy licencja Microsoft Copilot to 2 500 DKK, co daje różnicę rzędu 100x. Zmianę tę wspierają samorządy, takie jak gmina Aarhus, która wydała 42 mln DKK na licencje Microsoftu w 2024 r., a obecnie dąży do tego, by do 2030 r. 25 proc. jej pakietów biurowych opierało się na open source. Zgodnie z wyliczeniami gminy, inwestycja 3 mln DKK rocznie (w latach 2026–2029) w transformację, wygeneruje stałą nadwyżkę w wysokości 7 mln DKK rocznie już od 2029 roku. W tym modelu Dania świadomie akceptuje wyższe początkowe koszty szkoleń i wdrożeń, z twardym założeniem, że uniezależnienie się od opłat licencyjnych szybko zrekompensuje te nakłady.

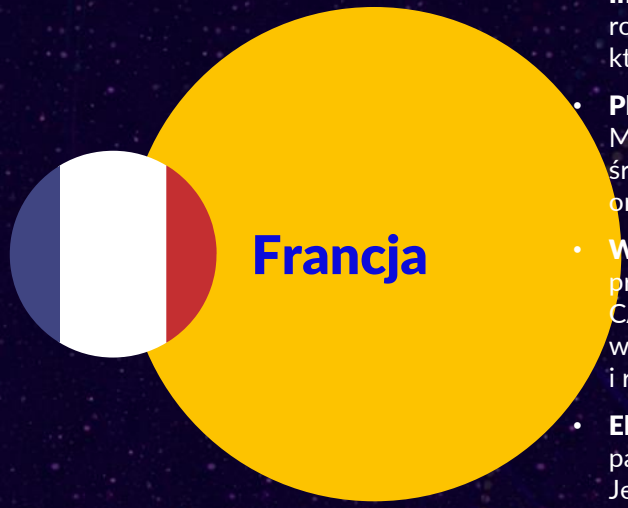


- **Współpraca z rynkiem i wsparcie ekosystemu GovTech** – duński model suwerenności technologicznej nie opiera się wyłącznie na działaniach administracji, lecz zakłada ścisłą współpracę publiczno-prywatną. Rząd aktywnie stymuluje rozwój lokalnych startupów i branży GovTech, wykorzystując do tego zamówienia publiczne, w tym preferencje dla MŚP zgodne z prawem unijnym, programy pilotażowe oraz otwarte dane publiczne, które napędzają innowacje. Dzięki inwestycjom w krajowy ekosystem – ze szczególnym uwzględnieniem cyberbezpieczeństwa, sztucznej inteligencji oraz wsparcia eksportu technologii – duńskie firmy mogą tworzyć rozwiązania bezpośrednio zasilające państwowe urzędy. Sztandarowym przykładem skuteczności tego partnerstwa publiczno-prywatnego jest strategiczna współpraca z firmą Netcompany, która sukcesywnie migruje aplikacje opieki państwowej (welfare-state) do krajowej chmury. Efektem tych działań, konsekwentnie preferujących lokalne i europejskie rozwiązania w łańcuchach dostaw, jest utrzymywanie już połowy systemów IT sektora publicznego fizycznie na duńskich serwerach.
- **Wspólnota OS2, OSPO i horyzontalne współdzielenie kodu** – unikalnym na skalę europejską rozwiązaniem w redukcji zależności od pozaeuropejskich gigantów technologicznych jest duńskie podejście do współdzielenia oprogramowania. Proces ten napędza stowarzyszenie OS2 (*Offentligt Digitaliseringsfællesskab*), które zrzesza gminy i instytucje publiczne, aby wspólnie, w modelu kooperatywnym, zamawiać, rozwijać i utrzymywać otwarte rozwiązania z myślą o oszczędnościach budżetowych. Wspólnota oferuje już 26 gotowych produktów otwarto źródłowych (m.in. system OS2kitos używany przez 81 gmin oraz OS2borgerPC przez 43 gminy), co drastycznie obniża koszty i gwarantuje publiczną współwłasność kodu. Państwo systemowo wspiera ten oddolny model, tworząc struktury i jednostki takie jak Open Source Program Offices (OSPO) oraz publikując w 2024 roku oficjalne wytyczne „Vejledning om brug af open source i den offentlige sektor". Dokument ten – oparty na architektonicznej zasadzie 2.3 nakazującej unikanie technologii zamkniętych – instruuje sektor publiczny, jak kupować i wdrażać open source, a całości dopełnia rygorystyczne traktowanie danych publicznych jako dobra wspólnego, które jest bezpiecznie hostowane na państwowej chmurze GovCloud (np. katalog Datavejviser oparty na systemie CKAN).
- **Redukcja zależności od big tech** - Dania konsekwentnie przechodzi od teorii do działania, systematycznie wycofując się z zamkniętych rozwiązań zagranicznych gigantów na rzecz otwartych, lokalnych i europejskich alternatyw. Sztandarowym przykładem jest ogłoszony w czerwcu 2025 r. pilotaż duńskiego Ministerstwa Cyfryzacji, zakładający całkowitą migrację z Microsoft Office 365 i systemów Windows na LibreOffice oraz Linuksa (początkowo na połowie, a docelowo na wszystkich stanowiskach), co ma radykalnie obniżyć ryzyka geopolityczne, prawne i bezpieczeństwa oraz ograniczyć zjawisko *vendor lock-in*. Analogiczne uchwały o uniezależnieniu się od amerykańskich dostawców podjęły największe samorządy, w tym Kopenhaga i Aarhus. Gmina Aarhus wyznaczyła sobie ambitny cel, aby do 2030 r. 25 proc. jej pakietów biurowych opierało się na oprogramowaniu open source.



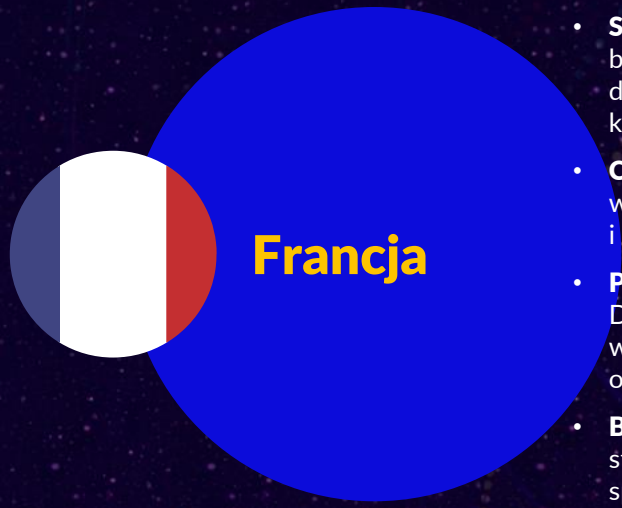
...

- **Suwerenność infrastrukturalna i kontrola cyfrowych węzłów** – duński model bezpieczeństwa opiera się na ścisłej, państwowej kontroli nad kluczowymi węzłami tożsamości i wymiany danych, które traktowane są jako infrastruktura krytyczna państwa. Fundamentem tego ekosystemu jest MitID – narodowy system e-tożsamości (zastępujący wcześniejszy NemID), służący obywatelom do logowania się do usług publicznych, bankowości oraz składania podpisów elektronicznych. Uzupełnia go platforma Digital Post, stanowiąca obowiązkowy i prawnie wiążący kanał komunikacji państwa z obywatelem, co radykalnie zmniejsza publiczną zależność od prywatnych platform komunikacyjnych. Płynny i bezpieczny obieg informacji zapewnia centralny portal Borger.dk oraz Data Distribution Platform, która pozwala na wymianę informacji między urzędami bez ich duplikowania. Państwo dba o to, by to ono, a nie komercyjni dostawcy, wyznaczało standardy interoperacyjności , zlecając m.in. otwarto źródłowe implementacje referencyjne (jak OIOSAML) oraz rozwijając własną chmurę państwową GovCloud, na której działa krajowy katalog danych (Datavejviser) oparty na systemie CKAN. Jednocześnie Dania stosuje bardzo pragmatyczną strategię chmurową: dopuszcza korzystanie z usług globalnych gigantów (np. AWS czy Google), ale pod twardym warunkiem fizycznej lokalizacji danych w Europie, pełnej zgodności z prawem UE i zachowania absolutnej kontroli państwa nad dostępem, co skutecznie zapobiega zjawisku vendor lock-in.
- **Cyberbezpieczeństwo, suwerenność danych i etyka jako znak jakości** – w obliczu stale utrzymującego się bardzo wysokiego poziomu zagrożeń szpiegowskich i cyberprzestępczych, Dania opiera swoją obronę na Narodowym Centrum Cyberbezpieczeństwa (CFCS), które aktywnie wykorzystuje algorytmy sztucznej inteligencji do monitorowania ataków (AI threat intelligence). Ochrona infrastruktury krytycznej i łańcuchów dostaw bazuje na ścisłej współpracy publiczno-prywatnej, inwestycjach w krajowy ekosystem cybernetyczny (MŚP, akademia) oraz rygorystycznym wdrażaniu duńskiej Ustawy o Cyberbezpieczeństwie, w pełni zintegrowanej z unijną dyrektywą NIS2. Równolegle państwo buduje swoją „suwerenność normatywną", kodując narodowe wartości – takie jak zaufanie i równość – w innowacyjne instrumenty rynkowe. Sztandarowym tego przykładem jest wprowadzenie unikalnego znaku etyki danych i cyberbezpieczeństwa (data-ethics/cyber seal). Instytucje i firmy spełniające wyśrubowane duńskie normy otrzymują oficjalny certyfikat zaufania, co buduje ich rynkową przewagę nad mniej przejrzystymi, globalnymi dostawcami. Dopełnieniem tej strategii jest polityka suwerenności danych, która zakłada bezpieczne udostępnianie otwartych danych publicznych do trenowania duńskich modeli AI, łącząc pełną zgodność z unijnymi standardami (jak AI Act) z silnym naciskiem na budowę narodowej odporności.
- **Ochrona obywateli danych i przed algorytmami** – Dania przesuwa ciężar suwerenności na bezwzględną ochronę jednostki przed wpływem algorytmów, wprowadzając regulacje często ostrzejsze niż standardy unijne. W walce z generatywną sztuczną inteligencją państwo znowelizowało prawo autorskie (2024/2025), przyznając każdemu obywatelowi pełne prawo do własnego wizerunku i głosu w starciu z deepfake'ami. Poszkodowani mogą żądać usunięcia treści i odszkodowania, a całkowity ciężar egzekwowania prawa oraz ryzyko wysokich kar finansowych przeniesiono bezpośrednio na platformy technologiczne. Równolegle, wzorując się na Australii, Kopenhaga szykuje na około 2026 rok ustawę zakazującą korzystania z mediów społecznościowych dzieciom poniżej 15. roku życia (z dopuszczeniem wyjątków od 13. roku życia za zgodą rodziców), aby chronić ich zdrowie psychiczne i wymusić na gigantach wdrożenie rygorystycznych systemów weryfikacji wieku. Tę prawną ochronę jednostki uzupełnia suwerenność normatywna – państwo promuje własne modele AI typu open source unikając rozwiązań zagranicznych , nagradza rzetelne podmioty oficjalną pieczęcią etyki danych (*Dataetisk Handelsmærke*) oraz wykorzystuje swoją nadchodzącą prezydencję w Radzie UE (II połowa 2025 r.), aby globalnie forsować surową odpowiedzialność platform za uzależniające algorytmy.

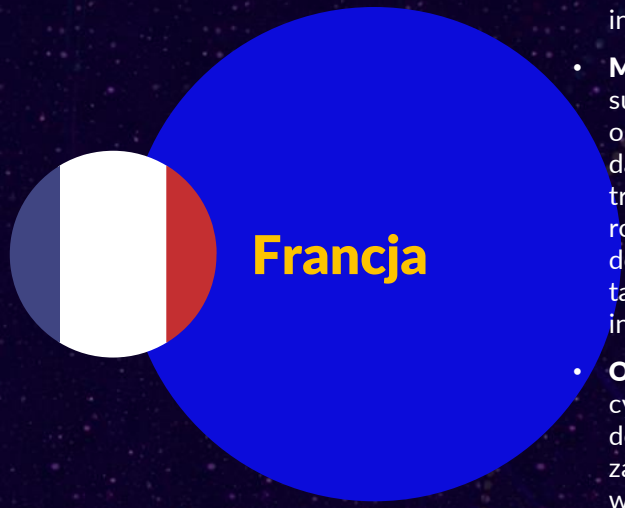


- **Kluczowe filary** – doktryna „Souveraineté Numérique” (suwerenność cyfrowa) jest we Francji traktowana jako nieodłączny element szerszej autonomii strategicznej państwa i Europy. Główne założenia to redukcja uzależnienia od USA i Chin, mocne promowanie własnych narodowych czempionów technologicznych oraz tzw. protekcjonizm cyfrowy w interesie europejskiej gospodarki.
- **Wizja suwerennej Europy** – dla Paryża prawdziwa suwerenność jest osiągalna tylko na poziomie Unii. Pod koniec 2025 roku Francja wraz z Niemcami ogłosiła tzw. Deklarację Berlińską, mającą na celu ujednolicenie unijnej definicji suwerenności, stworzenie europejskiego funduszu konkurencyjności oraz rozwój takich projektów jak europejski portfel tożsamości cyfrowej (EUDI Wallet).
- **Instytucje i koordynacja (DINUM i ANSSI)** – działania rządu centralizuje Międzyresortowa Dyrekcja ds. Cyfryzacji (DINUM), która pełni rolę głównego architekta infrastruktury państwowej. Jednocześnie ogromną, władczą rolę pełni agencja cyberbezpieczeństwa ANSSI, która narzuca niezwykle rygorystyczne wymogi i audyty dla technologii wykorzystywanych przez państwo.
- **Plan France 2030 (odpowiednik niemieckiej HighTech Agenda i Zukunftsfonds)** – gigantyczny program inwestycyjny prezydenta Macrona o wartości 54 miliardów euro. Jego celem jest głęboka reindustrializacja i uzyskanie niezależności w technologiach jutra. Ogromne środki płyną na powrót produkcji mikroprocesorów na terytorium Francji (we współpracy m.in. z STMicroelectronics), biotechnologię oraz na rozwój superkomputerów i technologii kwantowych.
- **Wsparcie i skalowanie krajowych liderów (Programy Next40 / French Tech 120)** – Francja nie pozostawia rozwoju innowacji przypadkowi. Rząd tworzy elitarny, wspierany państwowo indeks 40 oraz 120 najbardziej obiecujących scale-upów (wzorem giełdowego CAC40). Wytypowane firmy technologiczne otrzymują tzw. *fast-track* (szybką ścieżkę) w urzędach, dedykowanych opiekunów w ministerstwach, pomoc w pozyskiwaniu zamówień publicznych oraz ulgi, aby mogły błyskawicznie urosnąć do rangi „jednorożców” i rzucić wyzwanie gigantom z USA czy Chin.
- **Ekspansja i podbój rynków przez markę „La French Tech”** – zorganizowany, silnie dotowany przez państwo ruch i globalna marka parasolowa zrzeszająca francuski ekosystem innowacji. Posiada swoje oficjalne "ambasady" (huby) w ponad 100 miastach na całym świecie. Jej zadaniem jest agresywna dyplomacja technologiczna: promowanie francuskich rozwiązań za granicą, ułatwianie startupom wchodzenia na nowe rynki oraz przyciąganie do Francji zagranicznych talentów i inwestorów (m.in. przez specjalny, uproszczony program wizowy *French Tech Visa*).
- **Plan Tibi (Mobilizacja krajowego kapitału prywatnego)** – przełomowa, francuska odpowiedź na problem wykupywania europejskich technologii przez amerykańskie fundusze. Prezydent Macron i rząd skutecznie zmobilizowali największych krajowych inwestorów instytucjonalnych (banki, fundusze emerytalne, firmy ubezpieczeniowe) do wyłożenia miliardów euro (I etap: 6 mld EUR, II etap: 7 mld EUR) na lokalne fundusze VC w fazie późnego wzrostu (*late-stage / growth*). Dzięki temu francuskie firmy deep-tech mogą pozyskiwać gigantyczne rundy finansowania na globalne skalowanie, utrzymując swoją własność, patenty i siedziby we Francji.

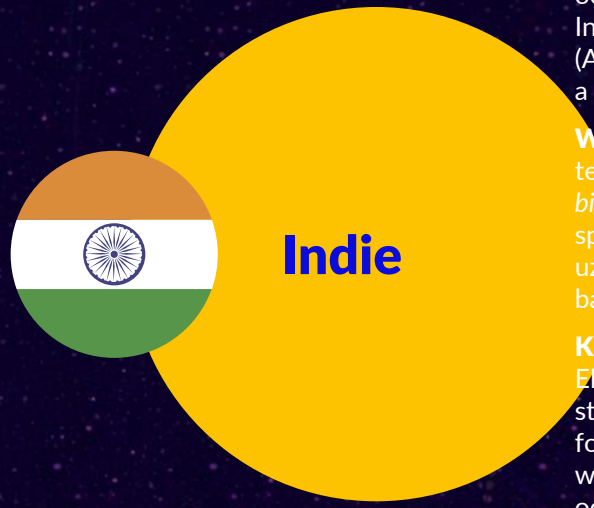
...



- **Protekcjonizm cyfrowy i preferencje „Made in Europe”** – rząd francuski jest głównym lobbystą w Unii Europejskiej na rzecz wprowadzenia zasady „Buy European Tech Act” w zamówieniach publicznych. Dąży do tego, by prawo unijne premiowało zakup rozwiązań informatycznych tworzonych w Europie, chroniąc rodzimy rynek przed tańszą lub zmonopolizowaną konkurencją z zewnątrz.
- **Współpraca z rynkiem i budowa czempionów** – Francja charakteryzuje się bardzo silnym interwencjonizmem państwowym. Administracja publiczna oraz państwowe fundusze celowo wybierają i gigantycznie dofinansowują wybrane krajowe podmioty (np. dostawcę chmury OVHcloud, startupy kwantowe jak Pascal czy firmy zajmujące się AI jak Mistral), aby mogły one konkurować na rynkach globalnych.
- **Strategia „Cloud de Confiance” (chmura zaufania)** – sformułowano francuską wizję suwerennej infrastruktury chmurowej. Zamiast budować chmurę państwową od zera, Francja zmusza globalnych graczy do tworzenia lokalnych partnerstw. Aby dostarczać usługi dla państwa, firmy takie jak Microsoft czy Google muszą wchodzić w spółki joint-venture z podmiotami francuskimi (np. Thales, Orange), które przejmują pełną kontrolę nad zarządzaniem serwerami i kluczami szyfrującymi na terenie Francji.
- **Certyfikacja SecNumCloud (ocena zgodności)** – jeden z najbardziej restrykcyjnych standardów bezpieczeństwa chmury na świecie, wydawany przez ANSSI. Każdy dostawca usług dla administracji i infrastruktury krytycznej musi udowodnić pełną separację prawną i operacyjną od prawodawstwa państw trzecich (w tym odporność na amerykański CLOUD Act wymuszający wydawanie danych).
- **Promocja open source w administracji** – Francja od lat konsekwentnie rozwija wykorzystanie otwartego oprogramowania (logiciels libres). DINUM publikuje zaktualizowane katalogi (SILL) zalecanego wolnego oprogramowania dla urzędów. Sztandarowym przykładem jest wdrożenie bezpiecznego, szyfrowanego komunikatora Tchap dla administracji państwowej, który zbudowano w całości w oparciu o otwarty protokół Matrix, omijając komunikatory korporacyjne.
- **Bezpieczeństwo infrastruktury krytycznej i łańcuchów dostaw** – w ramach strategii odporności Francja po cichu, ale niezwykle stanowczo, wprowadziła tzw. „ustawę Anti-Huawei”, która w praktyce de facto wymusiła na telekomach usunięcie i zablokowała sprzęt chińskich dostawców z kluczowych elementów sieci 5G.
- **Narodowa Strategia AI i Sovereign AI** – Francja inwestuje potężne środki, by stać się hubem sztucznej inteligencji w Europie. Państwo udostępnia potężne superkomputery (jak Jean Zay) darmowo lub na preferencyjnych warunkach dla badaczy i startupów, oraz mocno wspiera rozwój własnych, wielkich modeli językowych LLM o otwartym kodzie (jak globalny sukces firmy Mistral AI), aby uniknąć uzależnienia europejskiej gospodarki i nauki od modeli OpenAI czy Google.
- **Rozwój DPI (Digital Public Infrastructure)** - Francja bardzo mocno wspiera ogólnounijne wdrożenie EUDI Wallet, czyli bezpiecznego, zharmonizowanego systemu cyfrowej tożsamości, jako fundamentu interakcji obywateli z państwem.



- **Suwerenny pakiet biurowy LaSuite, w tym komunikator Visio czy Tchap** - w ramach budowania praktycznej suwerenności cyfrowej, Francja do 2027 roku planuje całkowicie wyeliminować z administracji państwowej i sektora nauki zagraniczne narzędzia korporacyjne (takie jak Microsoft Office 365, Teams czy Zoom). W ich miejsce wdrażany jest LaSuite – zintegrowany, bezpieczny pakiet biurowy rozwijany w modelu open source przez rządową agencję DINUM, którego kluczowym elementem jest komunikator wideo Visio. Rozwiązanie to gwarantuje pełną poufność przepływu informacji w państwie, ponieważ jest hostowane w certyfikowanej, krajowej chmurze (SecNumCloud od firmy Outscale) i wykorzystuje francuskie algorytmy sztucznej inteligencji do transkrypcji spotkań. Projekt, wspierany przez europejskie konsorcjum EDIC Digital Commons, jest już aktywnie wykorzystywany przez dziesiątki tysięcy urzędników, stanowiąc flagowy przykład udanego przejścia z uzależnienia od amerykańskiego Big Techu na w pełni kontrolowaną, suwerenną infrastrukturę cyfrową.
- **Migracja z pakietów Microsoft Office do francuskich rozwiązań w edukacji** – w ramach konsekwentnego budowania cyfrowej suwerenności, francuski region Île-de-France (obejmujący ok. 550 tysięcy uczniów i nauczycieli) stopniowo wycofuje ze szkół oprogramowanie Microsoft 365. Decyzja ta ma na celu zagwarantowanie pełnej zgodności z europejskim RODO, ochronę wrażliwych danych edukacyjnych przed amerykańskimi przepisami inwigilacyjnymi (takimi jak CLOUD Act czy FISA) oraz zablokowanie możliwości trenowania modeli AI na informacjach o uczniach. W miejsce zagranicznego Big Techu z powodzeniem wdrażane są certyfikowane, rodzime alternatywy: bezpieczna poczta od firmy Worldline, systemy zarządzania szkołą od Docaposte oraz suwerenny hosting dostarczany przez chmurę Leviia. Francuscy eksperci ds. cyberbezpieczeństwa z agencji ANSSI podkreślają, że choć transformacja ta wymaga czasu i inwestycji, to jest całkowicie wykonalna i stanowi kluczowy krok do odzyskania pełnej kontroli nad cyfrową infrastrukturą państwa przy jednoczesnym rozwijaniu lokalnego ekosystemu IT.
- **Ograniczenie dostępu do mediów społecznościowych dla dzieci i młodzieży** - ważnym elementem francuskiej walki o suwerenność cyfrową jest również ochrona najmłodszych obywateli przed wpływem globalnych platform. Francja wprowadziła przepisy ograniczające dostęp do mediów społecznościowych dla dzieci poniżej 15. roku życia (wymagające m.in. weryfikowalnej zgody rodziców). Zmuszając zagranicznych gigantów technologicznych (takich jak TikTok czy Instagram) do respektowania lokalnego prawa i wdrożenia systemów weryfikacji wieku, państwo aktywnie chroni wrażliwe dane nieletnich. Krok ten ma na celu ograniczenie wpływu uzależniających, pozaeuropejskich algorytmów na rozwój młodego pokolenia i udowadnia, że prawdziwa suwerenność to także zdolność narzucania własnych, twardych zasad funkcjonowania zagranicznemu Big Techowi.
- **Zakaz smartfonów w liceach, szkołach podstawowych czy gimnazjach** - kolejnym krokiem Francji w budowaniu cyfrowej higieny i niezależności środowiska edukacyjnego jest radykalne ograniczenie korzystania z prywatnych urządzeń mobilnych przez uczniów. Obowiązujący już wcześniej całkowity zakaz używania smartfonów w szkołach podstawowych i gimnazjach zostaje obecnie rozszerzony także na licea. Działanie to ma na celu nie tylko poprawę koncentracji i relacji rówieśniczych, ale przede wszystkim ochronę młodzieży przed uzależniającym wpływem algorytmów globalnych platform społecznościowych. Stanowi to naturalne uzupełnienie francuskiej polityki wyzwalania szkół spod wpływu zagranicznego Big Techu i odzyskiwania państwowej kontroli nad cyfrowym bezpieczeństwem najmłodszych obywateli.



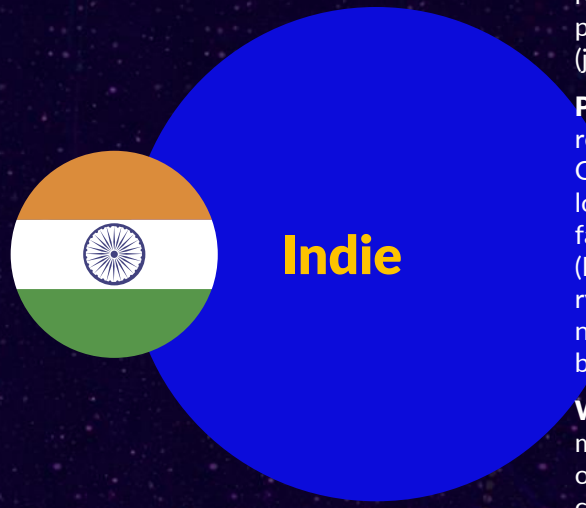
Indie

Kluczowe filary – „Atmanirbhar Bharat", DPI i technonacjonalizm - dla Indii, najludniejszego państwa i największej demokracji świata, suwerenność technologiczna to imperatyw strategiczny oparty na doktrynie „Atmanirbhar Bharat" (samowystarczalne Indie) oraz reindustrializacji gospodarki. Kraj ten realizuje koncepcję tzw. technonacjonalizmu – łączy globalną otwartość na kapitał z bezwzględną ochroną narodowych interesów i preferowaniem lokalnych rozwiązań. Absolutnym rdzeniem tej transformacji jest budowa Cyfrowej Infrastruktury Publicznej (DPI), znanej jako *India Stack*. W przeciwieństwie do zachodu, Indie traktują kluczowe rejestry tożsamości cyfrowej (Aadhaar), państwowe systemy płatności (UPI) czy e-dokumenty (DigiLocker) jako krytyczną, darmową infrastrukturę państwową, a nie komercyjne centra zysku kontrolowane przez prywatne korporacje.

Wizja suwerenności – „Trzecia droga", postkolonialna duma - Indie promują swoją strategię jako globalną „trzecią drogę" zarządzania technologiami w kraju. To precyzyjny balans (tzw. strategiczny *hedging*) pomiędzy amerykańskim modelem zdominowanym przez prywatny *big tech*, a zamkniętą, kontrolowaną autarkią technologiczną Chin. Wizja ta jest głęboko napędzana narracją postkolonialną. Rząd otwarcie sprzeciwia się kolonializmowi danych i kultury zachodu, podkreślając, że zagraniczne korporacje nie mogą traktować 850 milionów indyjskich użytkowników internetu jako darmowego źródła surowca dla AI. Celem Indii jest definitywne przejście od bycia jedynie cyfrowym „globalnym back-office" i konsumentem technologii, do roli jej aktywnego twórcy i hegemona wyznaczającego globalne standardy.

Koordynacja polityk i wdrożenia – MeitY, NITI Aayog i wyzwania fragmentacji - głównym architektem polityki państwa jest Ministerstwo Elektroniki i Technologii Informacyjnych (MeitY), którego gigantyczny budżet rok do roku rośnie o dziesiątki procent, finansując strategiczne misje w obszarze AI i mikroprocesorów. System wspiera silnie umocowany rządowy think-tank NITI Aayog (National Institution for Transforming India) wyznaczający ramy strategiczne np. AI w Indiach, publikując narodową strategię AI i koordynując inicjatywy w sektorach jak rolnictwo, zdrowie czy mobilność oraz wyspecjalizowane agencje wdrożeniowe: India Semiconductor Mission (ISM) odpowiedzialna za budowę fabryk chipów, ośrodek C-DAC projektujący superkomputery, czy agencja CERT-In, która nałożyła na działające w Indiach firmy najbardziej restrykcyjny na świecie, 6-godzinny wymóg raportowania incydentów cyberbezpieczeństwa. Piętą achillesową tego zjawiska pozostaje jednak fragmentacja biurokratyczna – polityki telekomunikacyjne i IT są rozsiane po wielu resortach, a poszczególne stany realizują nakładające się na siebie agendy.

...



Indie

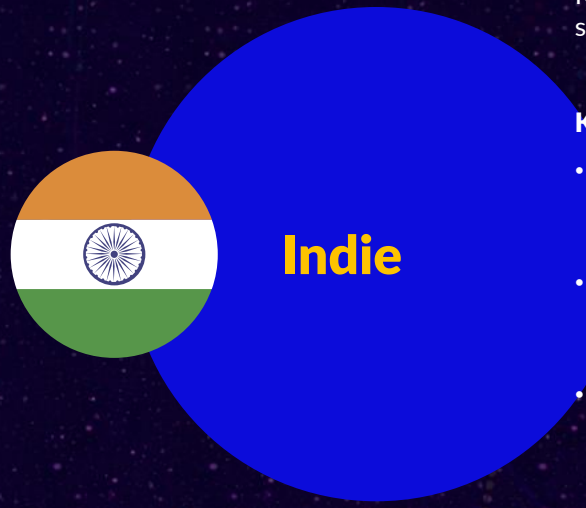
...

Finansowanie i strategie, ulgi – programy PLI, IndiaAI Mission i Anusandhan Fund - głównym rynkowym orężem Indii nie są tradycyjne ulgi na B+R, lecz system PLI (Production-Linked Incentive). Dysponujący pulą blisko 28 mld USD program na masową skalę subsydiuje 14 sektorów gospodarki, ale tylko w zamian za udowodniony przyrost fizycznej produkcji wewnątrz kraju – mechanizm ten już doprowadził do 146-procentowego wzrostu produkcji elektroniki. Ponieważ indyjskie wydatki na B+R są drastycznie niskie (poniżej 1% PKB), rząd uruchomił w 2025 r. gigantyczny, wart 12 mld USD fundusz Anusandhan Fund przeznaczony na badania deep-tech na uczelniach. Równolegle państwo realizuje duży program IndiaAI Mission (1,2 mld USD), dofinansowując m.in. zakup ponad 10 000 procesorów GPU, aby zaoferować rodzimym startupom tanią moc obliczeniową. Działania rządu uruchamiają dodatkowy kapitał prywatny – m.in. konglomerat Adani ogłosił plany inwestycji 100 mld USD do 2035 roku w suwerenną infrastrukturę AI i centra danych zasilane zieloną energią, a startupy deep-techowe (jak Neysa) pozyskują miliardowe rundy finansowania na rozbudowę krajowych klastrów obliczeniowych.

Preferencje dla lokalnych firm i zamówienia publiczne – Aplikacje "Swadeshi" i wymogi lokalizacji -Indie wdrożyły jeden z najbardziej rozbudowanych na świecie systemów wspierania lokalnego biznesu. W ramach inicjatywy „Make in India” (oraz przepisów Public Procurement Order), państwo faworyzuje aplikacje "Swadeshi" (rodzime), narzucając w wielu przetargach rządowych wymóg posiadania minimum 50% lokalnej zawartości (local content) oraz dopuszczając aż do 20% marży preferencyjnej dla indyjskich ofert.). W administracji państwowej faworyzuje się oprogramowanie i usługi tworzone w Indiach (np. pakiety biurowe firmy Zoho). Szczególny nacisk kładzie się na sektor obronny (DPP), gdzie wprowadzono cel osiągnięcia 70% sprzętu pochodzenia krajowego do 2027 r.. Ponadto, przepisy o ochronie danych wprowadzają rygorystyczne wymogi lokalizacji infrastruktury – zagraniczne firmy muszą fizycznie przechowywać i przetwarzać dane indyjskich obywateli na serwerach wewnątrz kraju, poddając się jurysdykcji indyjskich sądów (szczególnie w oparciu o indyjską ustawę IT, pozwalającą na twarde blokowanie treści). Państwo wymusza także na zagranicznym big techu sprawiedliwy podział zysków z lokalnymi twórcami.

Współpraca z rynkiem czyli publiczne tory, prywatne innowacje (ang. public rails, private innovation) i koncesjonowane PPP - Indyjski model kooperacji zakłada, że to rząd buduje i utrzymuje niekomercyjną, darmową bazową infrastrukturę, taką jak system identyfikacji obywateli (Aadhaar), protokół szybkich płatności (UPI) czy sieć e-commerce (ONDC). Są to otwarte protokoły i interfejsy (API), które stanowią cyfrowe dobro publiczne. Państwo dba o to, by te "tory" były tanie, bezpieczne, powszechnie dostępne i nie zależały od kaprysów prywatnych monopoli. Z kolei prywatne firmy budują na nich komercyjne usługi. Państwo nie próbuje tworzyć jedynej, słusznej aplikacji rządowej, z której obywatele muszą korzystać. Zamiast tego udostępnia wspomniane „tory” rynkowi. Prywatne firmy (od małych indyjskich startupów, przez banki, aż po zachodnich gigantów jak Google Pay czy Walmart PhonePe) budują swoje własne aplikacje, usługi i modele biznesowe w oparciu o tę darmową infrastrukturę. W krytycznych sektorach sprzętowych państwo opiera się na wspieranych miliardami modelach Joint Venture: to zagraniczny partner (np. tajwański PSMC lub amerykański Micron) musi dostarczyć rygorystyczne know-how technologiczne, a indyjski konglomerat (np. Tata Group) oraz państwo wnoszą kapitał i zyski z lokalnego rynku. Rząd otworzył na rynek prywatny również sektor kosmiczny (przez organizację IN-SPACe), umożliwiając startupom komercyjne wykorzystanie infrastruktury państwowej agencji ISRO.

...



...

Dyplomacja i eksport w którym DPI (ang. Digital Public Infrastructure) z Indii jest elementem budowy Globalnego Południa - Indie zmonetyzowały swój sukces wewnętrzny, przekształcając architekturę DPI w potężne narzędzie soft power – tzw. dyplomację fintechową. Narodowy system płatności natychmiastowych UPI (przetwarzający dziesiątki mld transakcji miesięcznie) jest już eksportowany i honorowany w ponad 8 państwach, w tym w Singapurze, ZEA czy we Francji. Podczas prezydencji w G20 Nowe Delhi przeforsowało stworzenie Globalnego Repozytorium DPI, umiejętnie pozycjonując Indie jako architekta otwartego, bezpiecznego systemu cyfrowego dla państw Globalnego Południa i stanowiąc realną, bezpieczną alternatywę dla opartych na długu chińskich inicjatyw Cyfrowego Jedwabnego Szlaku. Równolegle nowożytną dyplomację Indii wspiera gigantyczna, globalna diaspora technologiczna z Doliny Krzemowej, pełniąca rolę „mnożnika suwerenności", ułatwiająca transfer wiedzy, kapitału i patentów z powrotem do kraju.

KLUCZOWE TECHNOLOGIE I SEKTORY

- **Fintech i platformy DPI (*India Stack*)** - narodowe usługi oparte na otwartym kodzie np. e-tożsamość Aadhaar, e-dokumenty DigiLocker i platformy e-commerce (ONDC) – to infrastruktura wyceniana na 100 mld USD rocznej wartości dla gospodarki, eliminująca monopole *big tech*.
- **Półprzewodniki i ucieczka przed importem** - Indie importują ponad 65% procesorów. Aby to zmienić, w ramach wartych 9 mld USD dotacji z misji ISM 1.0 oraz 2.0 powstają pierwsze ogromne krajowe fabryki oraz zakłady testowania (OSAT), w tym gigantyczna inwestycja Tata Electronics w Dholera celująca w układy dla motoryzacji i telekomunikacji.
- **Suwerenne AI i otwarte modele** - zamiast rywalizować z OpenAI o moc obliczeniową dla największych LLM-ów, Indie aspirują do miana światowej stolicy wdrożeń AI (*Use Case Capital*). Rodzime platformy takie jak Bhashini, Krutrim czy Sarvam AI skupiają się na obsłudze głosowej i tekstowej 22 oficjalnych języków państwowych, zdecydowanie popularyzując dostęp do edukacji czy e-zdrowia dla obywateli. Państwo przy tym ogłasza konkursy na modele wspierając AI budowany przez rynek.
- **Komputery kwantowe i 6G** - narodowa Misja Kwantowa (NQM) z budżetem 730 mln USD inwestuje potężne środki w superbezpieczną komunikację (QKD), podczas gdy inicjatywa Bharat 6G wyznaczyła ambitny cel: Indie mają do 2030 r. posiadać 10 proc. globalnych patentów dla standardu 6G, by przestać być wyłącznie biorcą zagranicznych technologii telekomunikacyjnych.
- **Chmura MeghRaj i cyberbezpieczeństwo (BharOS)** - jako odpowiedź na fakt, że ponad 75% usług w chmurze w Indiach operuje na zagranicznej infrastrukturze, wdrażana jest państwowa chmura MeghRaj. Dla urzędników i agencji krytycznych stworzono także suwerenny, w pełni pozbawiony śledzenia mobilny system operacyjny BharOS, chroniący państwo przed wpływami zachodniego oprogramowania.

Izrael

Kluczowe filary suwerenności technologicznej tworzonej z konieczności jako fuzja cywilno-wojskowa z doktryną „Start-up Nation” – dla Izraela suwerenność technologiczna nie jest wyborem ideologicznym, lecz strukturalną koniecznością i absolutnym fundamentem fizycznego przetrwania na bliskim wschodzie oraz bezpieczeństwa narodowego. Zamiast dążyć do pełnej samowystarczalności (autarkii), kraj ten opiera swoją strategię na budowaniu asymetrycznej przewagi technologicznej, w tym jakościowej przewagi militarnej – QME, w strategicznych niszach, takich jak cyberbezpieczeństwo, sztuczna inteligencja, *deep tech* i technologie podwójnego zastosowania (ang. *dual-use*). Ten unikalny model, określany jako suwerenność poprzez przywództwo w innowacjach, napędzany jest głęboką fuzją sektora cywilnego i wojskowego. Kluczową rolę odgrywa tu armia (IDF), a zwłaszcza elitarna Jednostka 8200 wywiadu sygnałowego, która działa jako potężny inkubator innowacji, masowo transferując technologie i wyszkolonych ekspertów bezpośrednio do cywilnego ekosystemu komercyjnego (model z wojska do startupu czyli *IDF-to-startup*). Państwo aktywnie stymuluje rozwój „Startup Nation” poprzez bezpośrednie granty gotówkowe dla firm na badania i rozwój (zamiast standardowych ulg podatkowych), co winduje krajowe wydatki na B+R do rekordowego poziomu 6,3% PKB – najwyższego na świecie. Całość dopełnia budowany z pomocą państwa ekosystem funduszy VC, wsparty historycznym modelem Yozma, integrując ponad 430 międzynarodowych centrów B+R, przy jednoczesnym zachowaniu twardej kontroli nad narodową własnością intelektualną. Osiągnięcie statusu globalnego lidera sprawia, że eksport izraelskich technologii obronnych i z zakresu cyberbezpieczeństwa staje się potężną walutą dyplomatyczną, która zniechęca społeczność międzynarodową do izolacji kraju, uzależnia partnerów technologicznie i gwarantuje stabilne sojusze mocarstwowe.

Wizja narodowa i globalna sieć partnerstw – Izrael postrzega technologię nie jako gałąź biznesu służącą do zarabiania pieniędzy, ale ostateczny gwarant istnienia państwa i narodowej odporności (tzw. rezyliencji), zwłaszcza w warunkach wojennych i globalnego spowolnienia na rynku funduszy VC. Jeśli przewaga zostanie utracona, czyli Izrael straci swoją technologiczną przewagę, państwo może dosłownie przestać istnieć. Suwerenność w tym ujęciu nie oznacza izolacji, lecz budowę gęstej sieci partnerstw i pozycjonowanie państwa jako globalnego huba deep tech, zintegrowanego z ekosystemami USA i UE. Wyrazem tego podejścia jest ogłoszone w styczniu 2026 r. strategiczne partnerstwo z Waszyngtonem (obejmujące AI, technologie kwantowe i półprzewodniki), które czyni z Izraela bezpieczny węzeł („Pax Silica node”) w światowych łańcuchach dostaw. Państwo chroni się przed nadmierną zależnością od mocarstw (USA czy Chin) poprzez inwestycje w lokalną produkcję oraz potężną ofensywę eksportową. Zaawansowane technologie stanowią ponad 50 proc. całego eksportu kraju, a wiodącą rolę odgrywają w nim warte miliardy dolarów innowacje z zakresu cyberbezpieczeństwa – unikalne systemy, na których awarię świat nie może sobie dzisiaj pozwolić.

...

Izrael

...

Centralna koordynacja, ekosystem innowacyjny i Jednostka 8200 – architektura suwerenności technologicznej Izraela opiera się na unikalnej, ścisłej integracji agencji rządowych, sił zbrojnych i rynku prywatnego. Głównym architektem cywilnej polityki innowacyjnej jest Israel Innovation Authority (IIA), która dysponując rocznym budżetem rzędu miliarda dolarów, działa jako państwowy inwestor strategiczny i podmiot który ogranicza ryzyko inwestycyjne (risk mitigator), finansując rozwój technologii deep tech, kwantowych i AI w obszarach, gdzie prywatny kapitał jest zbyt ostrożny. Nad narodowym cyberbezpieczeństwem i ochroną infrastruktury krytycznej czuwa z kolei podlegająca bezpośrednio premierowi Israel National Cyber Directorate (INCD). Prawdziwym rdzeniem i bezprecedensowym inkubatorem izraelskiej potęgi technologicznej jest jednak wojsko i służby specjalne. Dyrekcja B+R Ministerstwa Obrony (MAFAT/DDR&D) oraz inicjatywy takie jak fundusz Libertad (uruchomiony przez Mosad) aktywnie integrują badania obronne z cywilną gospodarką, aby utrzymać jakościową przewagę militarną kraju (QME). Absolutnym centrum tego modelu jest elitarna Jednostka 8200 wywiadu wojskowego – jej absolwenci po zakończeniu służby masowo zakładają startupy (np. Check Point), zapewniając bezpośredni transfer najnowocześniejszej wiedzy z tajnego sektora do komercji. Mimo tych sukcesów, izraelski system boryka się ze słabą koordynacją horyzontalną – jak wykazał strategiczny raport Komitetu Nagela z 2025 roku, postulujący m.in. budowę potężnego narodowego superkomputera.

Mobilizowanie kapitału, Yozma 2.0 i globalna skala finansowania B+R – izraelski model opiera się na inteligentnym współdzieleniu ryzyka, co czyni z państwa aktywnego inwestora strategicznego, a nie tylko dawcę kapitału. Izrael wydaje na badania i rozwój (B+R) rekordowe w skali świata środki idące w dziesiątki miliardów dolarów rocznie. Fundamentem tego ekosystemu jest legendarny mechanizm Yozma, który w latach 90. dosłownie stworzył lokalny rynek venture capital poprzez państwowe współinwestowanie, gdzie w razie rynkowego sukcesu prywatni inwestorzy mogli tanio wykupić udziały rządu. Dziś ten model napędza program Yozma 2.0 (na lata 2024–2026), w którym państwo lewaruje własne środki (np. ok. 160 mln USD) dopłatami dla lokalnych inwestorów instytucjonalnych (w proporcji 0.3:1), by docelowo zmobilizować nawet 2 mld USD prywatnego kapitału. Zastrzyk ten obwarowany jest twardymi warunkami suwerennościowymi: fundusze muszą lokować 70 proc. środków w izraelskie firmy, z czego połowę w strategiczny obszar deep tech. System ten potęguje Israel Innovation Authority (IIA), która dostarcza startupom potężne finansowanie nierozwadniające (non-dilutive funding). IIA przyznaje bezpośrednie granty gotówkowe pokrywające od 20 do nawet 85 proc. kosztów najtrudniejszych faz projektów; jeśli projekt upadnie, państwo nie żąda zwrotu pieniędzy, traktując to jako koszt budowy narodowych kompetencji (zwrot zysków następuje tylko przy komercyjnym sukcesie). Efektem tych działań, uzupełnionych bilateralnymi funduszami z USA czy Koreą Południową, jest potężny bo szacowany na 8–10 mld USD rocznie rynek VC, odporny na globalne spowolnienia.

...

Izrael

Preferencje w zamówieniach publicznych, rygorystyczny offset i system ulg podatkowych – Izrael nie stosuje twardego protekcjonizmu, lecz wyrafinowany ekosystem miękkich preferencji chroniących rodzimy rynek co pozwala obchodzić reguły WTO, które koncentruje się na cłach. Państwo aktywnie wykorzystuje zamówienia publiczne jako tarczę – w przetargach dla wojska (IDF) i infrastruktury krytycznej obowiązuje nieformalna zasada „buy Israeli", a instytucje publiczne stosują system preferencji cenowych, pozwalający na wybór krajowej oferty nawet wtedy, gdy jest ona o 15 proc. droższa od zagranicznego konkurenta. Niezwykle potężnym mechanizmem jest także obowiązkowy offset gospodarczy - każda zagraniczna korporacja wygrywająca duży państwowy kontrakt zbrojeniowy lub infrastrukturalny musi zainwestować od 20 do 35 proc. jego wartości z powrotem w izraelską gospodarkę, zlecając lokalne prace B+R lub dokonując transferu technologii. Izraelskie startupy (często rozwijane przez weteranów z jednostki 8200) stają się w ten sposób pierwszymi dostawcami dla armii i wywiadu, co pozwala im testować rozwiązania w realnych warunkach operacyjnych. Popyt ten uzupełnia bezprecedensowy system zachęt i dotacji bo firmy mogą liczyć m.in. na 0 proc. CIT na dochody z własności intelektualnej (IP) przez 10 lat, ulgi w ramach tzw. IP Box (np. obniżona do 6 proc. stawka podatku od sprzedaży IP za granicę) oraz granty pokrywające do 50 proc. kosztów badań, które zwracane są z zysków dopiero po komercyjnym sukcesie. Wsparcie to jest obwarowane rygorystycznymi warunkami - beneficjenci grantów agencji IIA mają zakaz transferu IP za granicę bez zgody rządu, muszą prowadzić R&D i produkcję w kraju przez 5 lat, a fundusze z programu Yozma mają nakaz inwestowania minimum 70 proc. kapitału w spółki izraelskie. Dzięki tym barierom oraz twardym wymogom transferu wiedzy nakładanym na gigantów technologicznych (którzy założyli w Izraelu ponad 350 centrów badawczych), Kneset skutecznie zatrzymuje kluczowe talenty, kapitał oraz własność intelektualną we własnych granicach.

Ofensywa eksportowa i technologia jako karta przetargowa w dyplomacji – dla Izraela eksport zaawansowanych technologii, stanowiących ponad połowę całkowitego eksportu państwa, to nie tylko warunek gospodarczego przetrwania, ale potężne narzędzie *soft power*. Sercem tej ofensywy jest jeden z najsilniejszych na świecie ekosystemów cyberbezpieczeństwa (również do szpiegowania i inwigilacji obywateli), zintegrowany w innowacyjnych hubach, takich jak CyberSpark w Beer Szewie (tzw. cyfrowej stolicy Izraela). To tam fizycznie łączą się siły agencji rządowych, wojska, uniwersytetów i globalnych korporacji, by rozwijać nie tylko defensywne, ale przede wszystkim wysoce zaawansowane, ofensywne technologie cybernetyczne. Państwo agresywnie promuje te rozwiązania na świecie, a ich sprzedaż – podlegająca rygorystycznej kontroli Ministerstwa Obrony (DECA) – jest z premedytacją wykorzystywana jako współczesna waluta geopolityczna. Udostępnianie obcym rządom tych unikalnych, sprawdzonych w walce systemów (*battlefield-proven tech*) jest wyrafinowanym narzędziem zacieśniania relacji dyplomatycznych i wywiadowczych na całym świecie (otwierając drzwi m.in. do strategicznych sojuszy, takich jak Porozumienia Abrahamowe). Co istotne, popyt na te technologie rośnie nawet pomimo trwającej wojny, potwierdzając ostatecznie strategiczną niezastępowalność izraelskiego ekosystemu i jego odporność na zawirowania geopolityczne.

Izrael

...

Projekt Nimbus i wymuszona suwerenność w chmurze – zamiast budować własną chmurę od zera, Izrael przyjął specyficzny model współpracy z amerykańskimi big techami. Poprzez wielomiliardowy rządowy kontrakt na chmurę obliczeniową, znany jako „Projekt Nimbus", państwo zmusiło firmy Google i Amazon (AWS) do zbudowania fizycznych centrów danych na swoim terytorium i realizacji również zamówień dotyczących opracowania narzędzi, które posłużą do kontroli Palestyńczyków. Zgodnie z bezwzględnymi warunkami umowy, wszelkie informacje publiczne, wojskowe i administracyjne są przetwarzane lokalnie i podlegają wyłącznie izraelskiemu prawu. Kontrakt zawiera bezprecedensowe klauzule - amerykańscy giganci nie mogą odciąć Izraela od usług nawet pod presją bojkotów czy zmian politycznych, a także zostali zobowiązani do stworzenia tajnego mechanizmu ostrzegania rządu (tzw. „wink"), jeśli obce państwa i jurysdykcje zażądałyby dostępu do izraelskich danych. Firmy zobowiązały się zatem do tajnego systemu powiadamiania rządu Izraela np. poprzez przelewy pieniężne w określonej kwocie (kodującej kraj żądania, 1000-9999 szekli) w ciągu 24 godzin, jeśli obce państwo lub sąd zażąda dostępu do izraelskich danych.

Suwerenne AI, superkomputery i militarna fuzja – Izrael traktuje rozwój sztucznej inteligencji jako nową oś rywalizacji o niezależność, stawiając ją na równi z fizyczną obroną granic i dążąc do wejścia do elitarnej pierwszej piątki światowych potęg w tej dziedzinie. Opierając się na potężnym ekosystemie ponad 2200 specjalistycznych startupów , państwo realizuje wielomiliardowe strategie – na czele z Narodowym Programem AI – aby radykalnie zmniejszyć zależność od zagranicznych chmur obliczeniowych (takich jak AWS, Google Cloud czy Microsoft Azure), a tym samym zapobiec wyciekom wrażliwych danych i postępującej kolonizacji kulturowej Izraela przez USA. Fundamentem tych działań jest budowa narodowej mocy obliczeniowej. W styczniu 2026 roku uruchomiono gigantyczne projekty suwerennych superkomputerów zarządzanych przez państwową agencję IIA, obejmujące m.in. klaster rozwijany przez Nebius Group, który dzięki tysiącom najnowocześniejszych akceleratorów Nvidia Blackwell ma osiągnąć moc 16 000 petaflopsów przy budżecie około 140 mln dolarów.
Ta potężna infrastruktura służy nie tylko integracji AI w sektorze zdrowia czy systemach autonomicznych, ale przede wszystkim tworzeniu narodowych dużych modeli językowych (LLM) zoptymalizowanych pod język hebrajski. Co kluczowe dla izraelskiego modelu suwerenności, innowacje te są nierozerwalnie związane z wojskiem (model dual-use) – zaawansowane algorytmy są bezpośrednio i błyskawicznie wdrażane w armii do analizy wywiadowczej oraz precyzyjnego namierzania celów, jak w przypadku systemów bojowych Lavender i Gospel, a także do rozwoju w pełni autonomicznego uzbrojenia. Dzięki tak masowym inwestycjom, przekraczającym miliard dolarów w samym 2026 roku, analitycy przewidują, że do 2030 roku sztuczna inteligencja wyprzedzi cyberbezpieczeństwo, stając się absolutnie wiodącym towarem eksportowym Izraela.

...

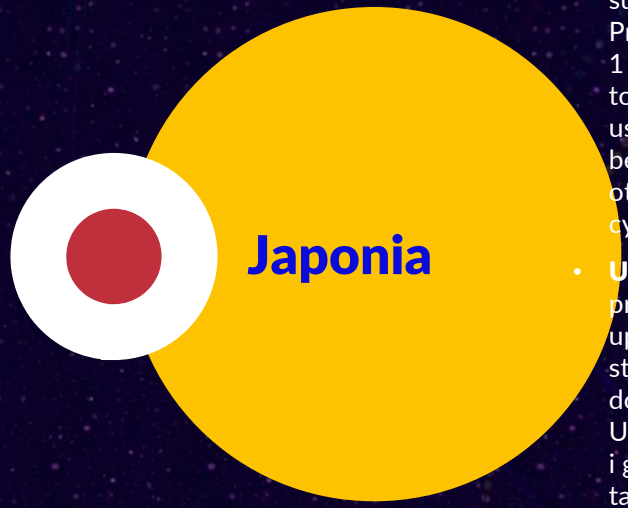
Izrael

...

Cyberbezpieczeństwo i zbrojeniowa samowystarczalność – Izrael wypracował pozycję absolutnego światowego lidera, kontrolując od 10 do 12 proc. globalnego rynku cyberbezpieczeństwa, co generuje potężny eksport rzędu 10–12 mld dolarów rocznie. Branża ta jest prawdziwym magnesem na kapitał – choć stanowi zaledwie 7 proc. lokalnego ekosystemu technologicznego, przyciąga blisko 40 proc. wszystkich izraelskich inwestycji VC (ok. 4 mld USD w 2024 r.), osiągając wolumen prywatnego finansowania równy 40 proc. całego rynku w USA. To stąd, często opierając się na talentach z wywiadu wojskowego (Unit 8200), wywodzą się globalni giganci tacy jak Check Point, CyberArk, Palo Alto Networks, Claroty czy startup Wiz, którego przejęcie przez Google w 2025 r. za 32 mld USD było największą akwizycją technologiczną w historii. Sercem tych innowacji jest m.in. narodowe centrum cyberbezpieczeństwa w Beer Szewie, zasilane inwestycjami rzędu 2 mld USD rocznie. Cyberbezpieczeństwo jest fundamentem nierozerwalnie łączącym się z fizyczną obronnością państwa. Historyczne embarga dawno temu wymusiły na Izraelu twardą samowystarczalność zbrojeniową (budując potęgę firm takich jak IAI czy Rafael), a dziś ta sama doktryna napędza walkę o pełną odporność łańcuchów dostaw (ang. *supply chain resilience*) w krytycznym obszarze półprzewodników i AI. Obecnie sektor ten wyznacza globalne trendy, strategicznie koncentrując się na zabezpieczaniu infrastruktury cyberfizycznej, systemach IoT oraz zwalczaniu zagrożeń napędzanych sztuczną inteligencją.

Półprzewodniki i krytyczne ogniwo globalnych łańcuchów dostaw – Izrael odgrywa strategiczną rolę w światowym ekosystemie układów scalonych, a eksport projektów półprzewodników rośnie w tempie 12,5 proc. rocznie, stanowiąc już 22 proc. całkowitego eksportu produktów technologicznych kraju. Zamiast ścigać się wyłącznie w masowej produkcji, państwo to stało się globalnym centrum projektowym (B+R) – na jego terytorium działa ponad 30 ośrodków badawczych gigantów takich jak Qualcomm czy Intel, dla którego Izrael jest flagowym miejscem projektowania chipów. Izraelskie fabryki (m.in. Tower Semiconductor) oraz lokalnie tworzona własność intelektualna (core IP) stanowią integralną część procesorów produkowanych w USA i Unii Europejskiej, obsługując 15 kluczowych węzłów globalnego łańcucha dostaw. Dowodem na tę strukturalną niezastępowalność jest ostatnia inwestycja Nvidii, która rozpoczęła budowę wartego miliardy dolarów kampusu w północnym Izraelu, który ma stać się fundamentem dla przyszłych centrów danych i zaawansowanych sieci napędzających rozwój sztucznej inteligencji.

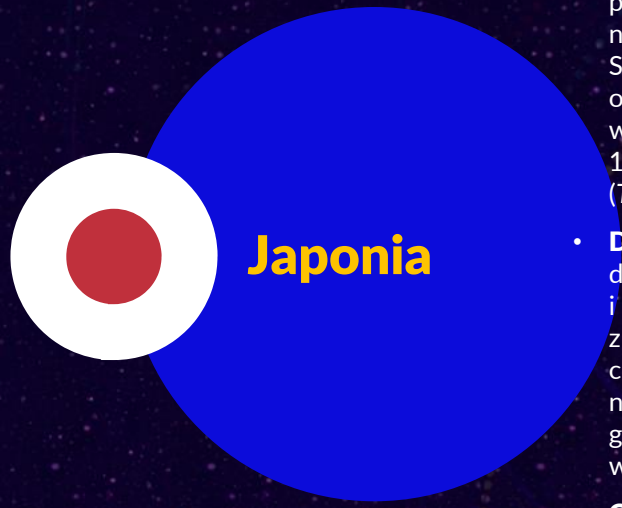
Technologie kwantowe i strategiczne partnerstwa – Izrael ambitnie nadrabia zaległości i dynamicznie rozbudowuje sektor komputerów kwantowych, traktując go jako kolejny, niezbędny filar swojej suwerenności technologicznej. Krajowy ekosystem badawczo-biznesowy rośnie w błyskawicznym tempie: tylko od 2025 roku liczba akademickich grup badawczych w tej dziedzinie skoczyła ze 144 do 240, a liczba specjalistycznych firm (takich jak rozwijające się Quantum Machines) wzrosła z 5 do 20. Aby sprostać gigantycznym kosztom i wyzwaniom technologicznym, państwo nie działa w izolacji, lecz mocno integruje się z globalnymi inicjatywami. Od października 2023 roku Izrael jest aktywnym członkiem europejskiego przedsięwzięcia EuroHPC JU (skupionego na superkomputerach i technologiach kwantowych), a równolegle zawiązał potężny sojusz ze Stanami Zjednoczonymi. W ramach tego partnerstwa oba kraje utworzą wspólne Centrum Sztucznej Inteligencji i Nauk Kwantowych o łącznej wartości 200 mln dolarów (każde z państw wniesie po 20 mln dolarów rocznie w latach 2026–2030), co ma trwale zabezpieczyć pozycję Izraela w nadchodzącej globalnej rewolucji kwantowej.



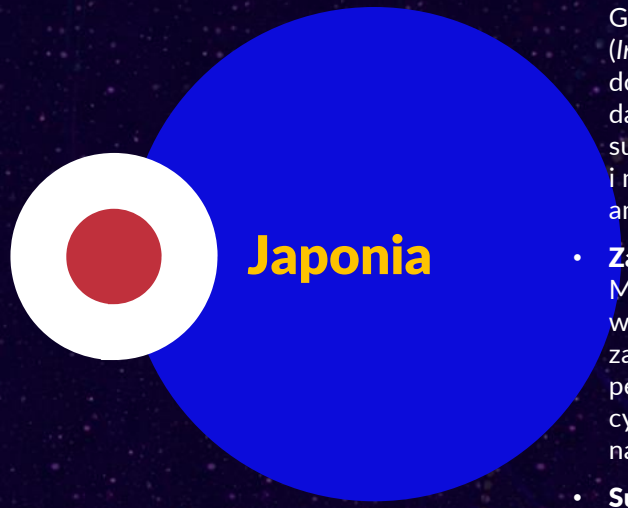
Japonia

- **Kluczowe filary – „Bezpieczeństwo Ekonomiczne", „Society 5.0" i „Strategiczna Niezbędność"** - dla Japonii, narażonej na wstrząsy geopolityczne, suwerenność technologiczna polega na nierozerwalnym łączeniu gospodarki z bezpieczeństwem narodowym (*Keizai Anpo*) w oparciu o wizję zaawansowanego cyfrowo społeczeństwa („Society 5.0"). Zamiast jawnego protekcjonizmu czy totalnej izolacji, Tokio stosuje doktrynę „małego podwórka, wysokiego płotu" (precyzyjna ochrona tylko ściśle wybranych, krytycznych technologii przy zachowaniu globalnej otwartości w pozostałych). Strategia ta jest dwutorowa: pierwszy tor to strategiczna autonomia (m.in. powrót produkcji półprzewodników i rozwój suwerennego AI), a drugi, najważniejszy tor to strategiczna niezbędność – agresywne i celowe inwestowanie w wąskie gardła globalnych technologii, aby stać się niezastąpionym ogniwem. Dzięki temu mocarstwa (jak USA czy Chiny) nie mogą uderzyć w japońskie interesy bez ryzyka zniszczenia własnych łańcuchów dostaw.
- **Centralna koordynacja (METI, Digital Agency i Minister ds. Bezpieczeństwa Ekonomicznego)** - japoński system zarządzania suwerennością opiera się na trzech potężnych filarach instytucjonalnych. Pierwszym z nich jest Ministerstwo Gospodarki, Handlu i Przemysłu (METI), które steruje polityką przemysłową oraz gigantycznymi inwestycjami w półprzewodniki i AI (z rocznym budżetem rzędu 1 bln JPY / ok. 6,5 mld USD na 2026 r.). Drugi filar to powołany w 2021 r. Minister ds. Promocji Bezpieczeństwa Ekonomicznego – to scentralizowany ośrodek decyzyjny zarządzający ryzykiem w łańcuchach dostaw, zapobiegający wyciekom technologii i wdrażający ustawę ESPA (obejmującą listę 17 krytycznych technologii). Dopełnieniem systemu jest utworzona w tym samym czasie, podległa bezpośrednio premierowi Agencja Cyfrowa (Digital Agency), która nadzoruje m.in. wdrożenie e-tożsamości *My Number*. Agencja ta otrzymała bezprecedensowe w japońskiej kulturze konsensusu uprawnienia ponad innymi resortami – może odgórnie narzucać standardy cyfrowe, a w przypadku opóźnień w transformacji danego resortu, ma prawo całkowicie przejąć i przekierować jego budżet IT.
- **Ustawa o Promowaniu Bezpieczeństwa Ekonomicznego (ESPA) – fundament prawny i narzędzie interwencji** - ten przełomowy akt prawny z 2022 roku (w pełni wdrożony w maju 2024 r.) stanowi główny oręż Japonii w walce o suwerenność, dając państwu potężne uprawnienia do ingerencji rynkowej. ESPA opiera się na czterech twardych filarach: (1) rygorystycznym zabezpieczeniu łańcuchów dostaw strategicznych komponentów, (2) systemowej ochronie infrastruktury krytycznej przed zagraniczną infiltracją, (3) gigantycznym dofinansowaniu przełomowych technologii oraz (4) unikalnym w japońskim systemie utajnianiu patentów o potencjale militarnym. Ustawa definiuje zamkniętą listę produktów krytycznych (m.in. półprzewodniki, programy chmurowe, roboty przemysłowe, akumulatory i gaz LNG), nakładając na kluczowe firmy obowiązek przedkładania do resortu METI „planów bezpieczeństwa dostaw". Zatwierdzenie takiego planu otwiera przedsiębiorstwom drogę do szerokiego wsparcia publicznego w postaci bezpośrednich dotacji oraz niskooprocentowanych pożyczek, co ma gwarantować Japonii stabilność technologiczną w warunkach globalnych kryzysów.
- **„Japan Growth Strategy Headquarters" i 17 sektorów strategicznych czyli powrót do państwowego sterowania gospodarką** – rząd premier Sanae Takaichi ogłosił nową doktrynę opartą na aktywnym wsparciu państwa, wyznaczając 17 priorytetowych obszarów (m.in. AI, półprzewodniki, energię fuzji oraz technologie kosmiczne), które otrzymają masowe, skoncentrowane inwestycje. Na czele nowo powołanego „Japan Growth Strategy Headquarters" stanęła osobiście premier, co nadaje tej instytucji najwyższą rangę polityczną i pozwala na błyskawiczne decyzje budżetowe. Strategia opiera się na dwóch filarach: „inwestycjach w zarządzanie kryzysowe", które mają uszczelnić łańcuchy dostaw, oraz „inwestycjach rozwojowych", mających zapewnić Japonii dominację w technologiach przyszłości.

...



- **Finansowanie innowacji i model publiczno-prywatny z rolą agencji NEDO oraz IPA** – Japonia nie tworzy jednego centralnego funduszu suwerenności, lecz operuje poprzez sieć wyspecjalizowanych agencji państwowych, które działają jak strategiczni inwestorzy technologiczni. Kluczową rolę odgrywa organizacja NEDO, finansująca przełomowe badania nad chipami i AI, oraz agencja IPA, która dzięki nowym uprawnieniom realizuje bezpośrednie zastrzyki kapitałowe, wkłady rzeczowe i gwarancje kredytowe dla producentów sprzętu. W ramach nowej polityki państwo zobowiązało się wyłożyć ponad 66 mld USD środków publicznych do 2030 roku, co ma zmobilizować gigantyczny kapitał prywatny i przynieść łączne inwestycje w japoński sektor wysokich technologii rzędu 330 mld USD w ciągu dekady.
- **Preferencje krajowe w przetargach, „miękki" protekcjonizm i wsparcie MŚP** – Japonia, podobnie jak Korea Południowa, nie stosuje jawnych przepisów typu „Kupuj Japońskie" (ze względu na umowy WTO GPA), lecz opiera się na wyrafinowanym systemie faktycznych preferencji. Kluczowym narzędziem jest certyfikacja ISMAP, która choć formalnie dostępna dla wszystkich, w przetargach na obsługę najbardziej wrażliwych danych rządowych tworzy środowisko faworyzujące krajowych operatorów, takich jak Sakura Internet czy NTT. System ten uzupełnia mechanizm „Buy Japan Implicit", sugerujący udział 20-30% lokalnych komponentów w kontraktach rządowych, oraz certyfikacje techniczne (MIC/TELEC), które skutecznie blokują dostawców wysokiego ryzyka. Równolegle państwo agresywnie wspiera sektor MŚP i deep-tech poprzez programy takie jak J-Startup czy Moonshot R&D (z budżetem 1 bln JPY), identyfikując ponad 1000 narodowych czempionów. Firmy te korzystają z ulg podatkowych na B+R sięgających 50% oraz statusu „zaufanego dostawcy" (*Trusted Vendor List*), co daje rodzimym graczom (np. Fujitsu, NEC) trwałą przewagę na rynku publicznym.
- **Dyplomacja technologiczna, sojusze demokratyczne i „friendshoring"** – w przeciwieństwie do modelu chińskiego, Japonia nie dąży do całkowitej izolacji i samowystarczalności, lecz opiera swoje bezpieczeństwo na niezastępowalności w globalnym łańcuchu wartości i gęstej sieci partnerstw. Tokio aktywnie uczestniczy w sojuszu Chip 4 (z USA, Koreą Płd. i Tajwanem), zacieśnia współpracę cyfrową z UE oraz koordynuje z USA i Holandią kontrolę eksportu zaawansowanych technologii, aby blokować postępy Chin w obszarach AI czy kwantów. Równolegle państwo realizuje strategię „friendshoringu", dosłownie „kupując" i przenosząc zagraniczną infrastrukturę na własne terytorium, aby uodpornić się na ewentualną blokadę Tajwanu. Zamiast rozwijać technologie od zera, japoński rząd przekazał gigantyczne wielomiliardowe subwencje (pokrywające blisko 50% kosztów) na budowę nowoczesnych fabryk tajwańskiego TSMC w Kumamoto oraz amerykańskiego koncernu Micron w Hiroszimie.
- **Odrodzenie półprzewodników – Projekt Rapidus, TSMC i „Hokkaido Valley**" - to najbardziej kapitałochłonny filar japońskiej suwerenności, na który od 2022 roku przeznaczono ponad 25,7 mld USD (najwyższy na świecie nakład w relacji do PKB). Strategia ta opiera się na dwóch filarach: sprowadzeniu tajwańskiego giganta TSMC do Kumamoto (joint venture JASM z udziałem Sony i Toyoty, wsparte dotacjami rzędu 1 bln JPY) oraz powołaniu narodowego czempiona – spółki Rapidus. Rapidus, wspierany przez osiem potężnych japońskich korporacji (m.in. Denso, Kioxia, SoftBank, Toyota) oraz agencję NEDO, otrzymał ponad 11 mld USD na przełomowy cel. To ominięcie technologicznej luki i uruchomienie do 2027 roku masowej produkcji najnowocześniejszych układów 2nm na wyspie Hokkaido. Wokół fabryki w Chitose powstaje „Hokkaido Valley" – strategiczny ekosystem wzorowany na Dolinie Krzemowej, który ma przywrócić Japonii status globalnej potęgi (cel: powrót do 10% udziału w rynku światowym) i zagwarantować dostęp do procesorów niezbędnych dla AI, robotyki oraz autonomicznej jazdy.

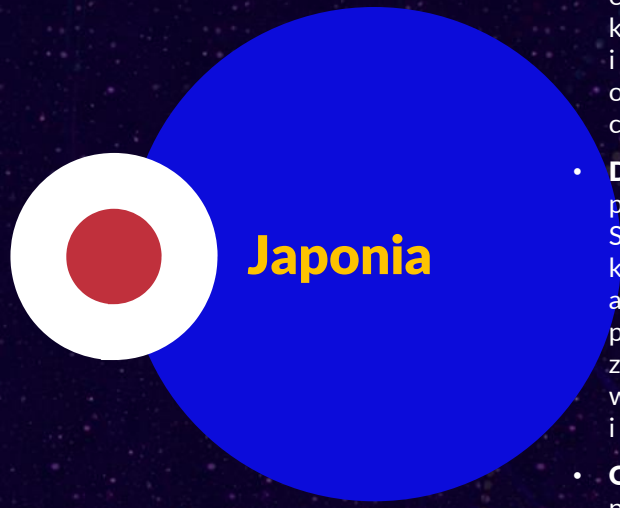


Japonia

...

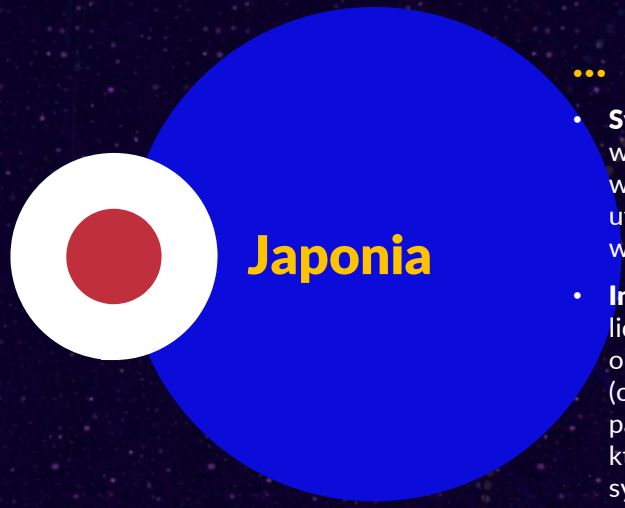
- **Strategia wąskich gardeł (ang. *choke points*) i materiałów zaawansowanych** - Japonia jest absolutnym i niekwestionowanym hegemonem w tzw. "upstreamie" przemysłu półprzewodnikowego mając ponad 60% rynku. Japońskie firmy (takie jak Shin-Etsu, SUMCO, JSR czy Tokyo Electron) kontrolują większość globalnego rynku wafli krzemowych, kluczowych żywic (fotorezydentów) używanych w litografii EUV oraz specjalistycznych maszyn. Państwo traktuje ten oligopol jako swoją najsilniejszą broń geopolityczną, ściśle dotując ten sektor i chroniąc go przed wrogimi przejęciami z zewnątrz. Podobnie Japonia podchodzi do robotyzacji, gdzie przyjęto cel posiadania 50% udziałów w rynku robotów przemysłowych (Fanuc, Yaskawa).
- **Suwerenna chmura rządowa GovCloud i Sakura Internet czyli systemowa detronizacja big tech** - Japonia dokonała historycznego zwrotu w polityce przechowywania danych państwowych, odchodząc od dotychczasowej dominacji amerykańskich gigantów (Amazon, Microsoft, Google, Oracle). Fundamentem tej zmiany jest wdrożenie zasady „Cloud First" oraz rygorystycznego programu certyfikacji ISMAP (*Information System Security Management and Assessment Program*). Kluczowym momentem było oficjalne nadanie statusu certyfikowanego dostawcy pierwszej czysto japońskiej firmie – Sakura Internet z Osaki. Agencja Cyfrowa wybrała ten podmiot do obsługi wrażliwych danych rządu i samorządów, wspierając go kontraktami o wartości ok. 100 mld JPY oraz gigantycznymi dotacjami z METI na budowę suwerennych centrów danych na Hokkaido. Celem strategicznym jest migracja 100% krytycznych danych administracji, służby zdrowia i ministerstw do 2028 roku do infrastruktury krajowej, która znajduje się pod japońską jurysdykcją i pozostaje całkowicie poza zasięgiem amerykańskich praw eksterytorialnych (np. *U.S. CLOUD Act*).
- **Zasada „Cloud-First" i modernizacja e-administracji** – system MyNumber oraz Mynaportal - japońska strategia „Wizja Cyfrowego Narodu Miasta-Ogród" (*Digital Garden City Nation Vision*) wraz z inicjatywą GovCloud zakładają głęboką modernizację usług publicznych oraz wdrożenie administracji opartej na sztucznej inteligencji. Kluczowym filarem cyfrowej tożsamości obywateli jest system MyNumber – zaawansowany odpowiednik numeru PESEL z mObywatel z funkcjami e-dowodu – zintegrowany z aplikacją Mynaportal, która umożliwia pełny dostęp do usług rządowych bezpośrednio ze smartfona. Rozwiązanie to ma docelowo stać się fundamentem suwerennej tożsamości cyfrowej Japończyków, funkcjonalnie zbliżonym do standardów europejskiego portfela tożsamości cyfrowej (*EUDI Wallet*), co pozwoli na bezpieczne i sprawne zarządzanie sprawami urzędowymi w sytuacjach kryzysowych.
- **Suwerenność danych i dyplomacja cyfrowa – koncepcja DFFT oraz znowelizowana ustawa APPI** - Japonia dysponuje rozbudowanym systemem ochrony informacji (*Act on the Protection of Personal Information – APPI*), który po nowelizacji z 2022 roku nakłada kary do 1 mld JPY za naruszenia i de facto wymaga lokalizacji danych rządowych oraz krytycznych na terytorium kraju. W kontekście suwerenności Tokio promuje koncepcję DFFT (ang. *Data Free Flow with Trust* czyli swobodny przepływ danych w oparciu o zaufanie), forsując ją na forach G7 i OECD jako globalną alternatywę dla chińskiego rygorystycznego podejścia do obrotu danymi cyfrowymi oraz europejskiego RODO. Strategia ta dąży do stworzenia systemu, w którym dane płyną swobodnie między państwami demokratycznymi w celu wspierania innowacji (AI), ale przy zachowaniu twardych, japońskich standardów bezpieczeństwa. W praktyce, poprzez wymogi certyfikacji ISMAP, Japonia premiuje operatorów posiadających centra danych na własnym terytorium, co pozwala na pełną integrację wrażliwych informacji (zdrowie, podatki) w ramach suwerennego ekosystemu My Number, chronionego przed ingerencją obcych jurysdykcji.

...



Japonia

- **Strategia AI i Suwerenna AI – „AI Basic Plan", własne modele LLM i potęga obliczeniowa** - Japonia dąży do zbudowania pełnej niezależności od amerykańskich i chińskich systemów AI, aby zapobiec tzw. cyfrowej kolonizacji kulturowej. Zatwierdzony w grudniu 2025 roku „Pierwszy Podstawowy Plan AI" oraz ustawa „Basic AI Act" zakładają zainwestowanie co najmniej 65 miliardów USD do 2030 roku w krajowe modele fundamentowe, centra danych i dedykowane procesory NPU rozwijane przez spółkę Rapidus. Kluczowym elementem strategii jest tworzenie czysto japońskich modeli językowych, takich jak opracowany przez NTT model „tsuzumi", który umożliwia bezpieczną pracę n własnym urządzeniu bez dostępu do internetu (tzw on-premise), czy rozwijany przez Fujitsu i NEC Fugaku-LLM, trenowany na unikalnych, lokalnych zbiorach danych. Aby zapewnić startupom i naukowcom niezbędną moc obliczeniową, rząd udostępnia narodową infrastrukturę w postaci superkomputerów Fugaku oraz zmodernizowanego systemu ABCI 3.0, co ma zagwarantować, że japońska sztuczna inteligencja będzie odzwierciedlać narodowe wartości i standardy bezpieczeństwa.
- **Dominacja w technologiach kwantowych, kosmicznych i obronnych – program Q-LEAP, JAXA oraz projekt GCAP** - Japonia postrzega przestrzeń kosmiczną i kwanty jako krytyczne pola walki o suwerenność, w które inwestuje rekordowe środki. W ramach Narodowej Strategii Kwantowej (budżet 1 bln JPY) oraz inicjatywy **Q-LEAP**, państwo – pod wodzą instytutu RIKEN – dąży do stworzenia komputerów kwantowych o mocy powyżej 1000 kubitów do 2030 roku, by uniknąć zależności od technologii USA i Chin. W domenie kosmicznej agencja **JAXA** zapewnia krajowi w pełni niezależny dostęp do orbity dzięki nowej generacji rakiet nośnych **H3** oraz buduje status globalnej potęgi poprzez udział w programie eksploracji Księżyca Artemis Accords. Ta technologiczna niezależność jest nierozerwalnie połączona z rekordowymi wydatkami na obronność (55 mld USD na 2026 r.), które finansują m.in. projekt **GCAP** (budowę myśliwca 6. generacji we współpracy z UK i Włochami) oraz rozwój autonomicznych dronów bojowych AI, co ma zagwarantować Japonii przewagę operacyjną i bezpieczeństwo ekonomiczne w niestabilnym regionie Indo-Pacyfiku.
- **Ochrona infrastruktury krytycznej i „cicha czystka" dostawców, ustawa ESPA oraz audyty łańcuchów dostaw** – Japonia, wzorem wielu państw, wprowadziła rygorystyczny nadzór nad 14 strategicznymi sektorami gospodarki (m.in. energetyką, finansami i telekomunikacją) w celu usunięcia ryzykownego sprzętu z infrastruktury państwa. Na mocy ustawy ESPA z 2022 roku (rozszerzonej w 2026 r.), dostawcy muszą przechodzić wieloetapową weryfikację bezpieczeństwa, co w praktyce pozwala na systemowe i ciche wypieranie chińskich gigantów (Huawei, ZTE) oraz producentów chipów „wysokiego ryzyka" bez konieczności wydawania oficjalnych zakazów. Strategia ta, oparta na koncepcji *Supply Chain Resilience*, wymusza m.in. obowiązkowe stosowanie 30% krajowych komponentów w przetargach rządowych. Zamiast gwałtownego odcięcia od Chin, Tokio stawia na ostrożną identyfikację zagrożeń i ochronę sektorów strategicznych, co pozwala na zachowanie cyberbezpieczeństwa przy jednoczesnym uwzględnieniu głębokich powiązań gospodarczych w regionie.



Japonia

...

- **System Utajniania Patentów (Patent Secrecy System)** - aby zapobiec transferowi kluczowych technologii do rywali (głównie Chin), w maju 2024 r. w ramach ESPA wprowadzono rewolucyjny system ochrony własności intelektualnej. Jeśli wniosek patentowy dotyczy wynalazków podwójnego zastosowania (np. zaawansowana broń, komunikacja kwantowa, fuzja jądrowa, stealth), państwo ma prawo go utajnić. Informacje o wynalazku nie są publikowane na świecie, a twórcy otrzymują bezwzględny zakaz udostępniania wiedzy za granicą w zamian za państwową rekompensatę finansową odpowiadającą potencjalnym stratom z komercjalizacji.
- **Infrastruktura komunikacyjna, strategia „Beyond 5G", lider 6G i bezpieczeństwo kwantowe** – Japonia dąży do objęcia pozycji globalnego lidera w standardach łączności kolejnej generacji, traktując to jako fundament suwerenności cyfrowej. Rząd, we współpracy z narodowymi operatorami (NTT, KDDI, SoftBank, Rakuten), realizuje strategię „Beyond 5G" z 2024 roku, na którą przeznaczono m.in. 200 mld JPY (ok. 1,3 mld USD). Celem jest ustanowienie japońskich patentów jako światowych standardów 6G przed 2030 rokiem. Równolegle państwo buduje systemy komunikacji kwantowej, nadzorowane przez Narodowe Laboratorium Nauk Kwantowych i instytut RIKEN, które mają zapewnić całkowitą odporność na podsłuch. Bezpieczeństwo tej infrastruktury domyka National Cyber Center, które systemowo blokuje zagraniczne „backdoory" i promuje autonomiczne sieci rządowe budowane przez NTT, eliminując ryzyko infiltracji przez obce służby wywiadowcze.

Korea Południowa

- **Kluczowe filary – „Digital Platform Government”** - dla tego niewielkiego terytorialnie, ale potężnego gospodarczo kraju technologia jest kwestią przetrwania. Korea traktuje suwerenność cyfrową jako bezwzględną zdolność państwa do kontrolowania strategicznych technologii oraz danych. Fundamentem jest *koncepcja Digital Platform Government* – integracja wszystkich usług publicznych w jednej, narodowej infrastrukturze. Priorytetem jest całkowita suwerenność danych, rozwój własnego sprzętu, w tym półprzewodników i pamięci, sztucznej inteligencji, rozwój cyberbezpieczeństwa oraz dominacja koreańskich firm na rynkach globalnych.
- **Centralna koordynacja (Ministerstwo Nauki i ICT)** - za realizację strategii w zakresie suwerenności technologicznej odpowiada Ministerstwo Nauki i ICT. Jest to centralny i duży ośrodek decyzyjny koordynujący gigantyczne programy finansowania, rozwój sztucznej inteligencji, infrastruktury cyfrowej oraz przemysłu półprzewodników. To tam zapadają decyzje o kształcie cyfrowej administracji państwowej.
- **Mapa Drogowa do 2028 r. (finansowanie deep-tech)** - rząd działa jak potężny inwestor technologiczny. W czasie ostatnich kilkunastu miesięcy przyjęto tzw. petycję międzyresortową, zakładającą bezpośrednie, państwowe inwestycje rzędu **23 miliardów USD** w rozwój 12 kluczowych obszarów (m.in. biotechnologię, obronność w kosmosie, robotykę). Państwo aktywnie współinwestuje z prywatnym kapitałem (fundusze VC, banki rozwoju), aby wspierać skalowanie innowacyjnych startupów.

...

Korea Południowa

- **Miękki protekcjonizm i preferencje dla firm krajowych w Korei Południowej** - Korea Południowa stanowi modelowy przykład państwa, które skutecznie chroni swój rynek zamówień publicznych i buduje suwerenność technologiczną bez otwartego łamania międzynarodowych umów handlowych (takich jak porozumienie WTO GPA). Ponieważ Seul nie może oficjalnie wprowadzić przepisów typu „Buy Korean", opiera się na strategii tzw. miękkiego protekcjonizmu przemysłowego (*soft protectionism*). Jest to wyrafinowany system barier regulacyjnych, standardów technicznych oraz ukrytych preferencji, który de facto zamyka dostęp do rynku publicznego przed zagranicznymi korporacjami. Głównym narzędziem tego systemu jest parasol ochronny rozpostarty nad małymi i średnimi przedsiębiorstwami (MŚP). Na mocy specjalnych ustaw (w tym *Act on Facilitation of Purchase of Small and Medium Enterprise-Manufactured Products oraz Software Industry Promotion Act*) gigantyczna część publicznych przetargów IT jest prawnie zarezerwowana wyłącznie dla mniejszych, lokalnych graczy. Ponieważ globalne korporacje są klasyfikowane jako duże przedsiębiorstwa i mogą startować jedynie w przetargach o wartości powyżej 220 tys. USD (których jest zdecydowanie mniej), są one systemowo odcinane od większości lukratywnego rynku. Wymusza to na zachodnich firmach kosztowne zakładanie lokalnych spółek lub konieczność dzielenia się zyskami z koreańskimi integratorami systemów. Najpotężniejszą barierą wejścia w obszarze nowoczesnych technologii jest jednak rygorystyczny system certyfikacji chmurowej CSAP (*Cloud Security Assurance Program*). Aby świadczyć usługi dla koreańskiej administracji, dostawca musi zagwarantować fizyczną separację danych, lokalizację centrów danych na terytorium kraju oraz całkowicie oddzielną infrastrukturę dla sektora publicznego. Dla globalnych gigantów z USA, których biznes opiera się na współdzieleniu zasobów chmurowych, tworzenie wyizolowanej "koreańskiej wersji" usług jest często technicznie i finansowo nieopłacalne, co wyklucza ich z systemów średniego i wysokiego poziomu bezpieczeństwa. Podobne utrudnienia dotyczą sprzętu IT i telekomunikacyjnego, który pomimo posiadania międzynarodowych atestów, musi przechodzić dodatkowe, przedłużające proces testy w koreańskich laboratoriach państwowych. Ten narodowy ekosystem domykają specyfikacje przetargowe, które urzędy często modyfikują i dopasowują pod możliwości techniczne krajowych producentów. Ponadto, w strategicznym sektorze obronnym obowiązuje absolutny priorytet dla sprzętu krajowego – import dopuszcza się tylko w przypadku braku lokalnego odpowiednika, zazwyczaj wymuszając przy tym transfer technologii lub tworzenie joint venture. Z kolei na etapie skalowania biznesu, rząd wspiera lokalnych liderów poprzez program G-PASS. Obejmuje on ponad tysiąc koreańskich firm, które zyskują status "zaufanego dostawcy", co nie tylko gwarantuje im priorytet w krajowej administracji, ale też zapewnia państwowe wsparcie w globalnej ekspansji.
- **K-Semiconductor Strategy (sojusz z czebolami)** - półprzewodniki to fundament suwerenności Korei. Rząd prowadzi największy w historii kraju program inwestycyjny, zakładający wpompowanie ponad **450 miliardów USD do 2030 roku** w budowę tzw. *Korean Semiconductor Belt*. Unikalną cechą tego modelu jest ścisła współpraca państwa z wielkimi konglomeratami (tzw. chabolami), takimi jak Samsung Group, SK Group czy LG. Celem jest utrzymanie globalnego monopolu w pamięciach DRAM i NAND oraz zabezpieczenie całego łańcucha dostaw.
- **Nowa ustawa K-Chips Act** - aby chronić swój przemysł przed działaniami USA i Chin, państwo wprowadziło bezprecedensową ustawę, która gwarantuje gigantom technologicznym (takim jak Samsung i SK Hynix) potężne zniżki podatkowe i granty na nakłady inwestycyjne w produkcję sprzętową, obowiązujące aż do 2032 roku.

Korea Południowa

...

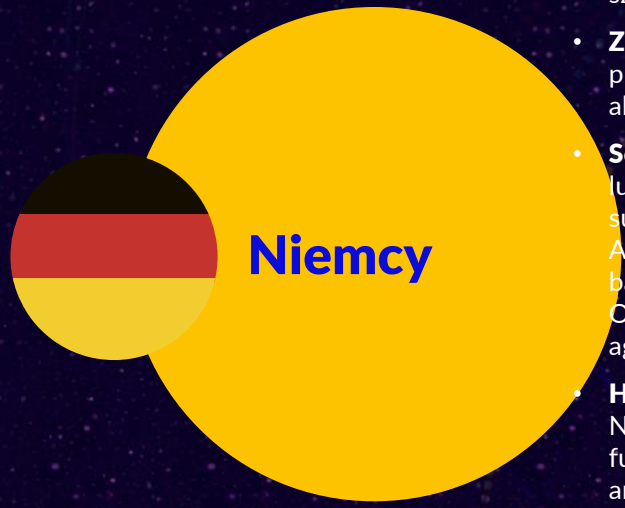
- **Program K-Cloud i własne procesory AI** - w 2023 r. uruchomiono program *K-Cloud*, którego celem jest stworzenie suwerennej infrastruktury chmurowej zoptymalizowanej pod sztuczną inteligencję. Projekt ten uniezależnia kraj od amerykańskich układów scalonych, ponieważ zakłada budowę supercentrów danych opartych wyłącznie o rozwijane w Korei własne procesory AI (tzw. NPU).
- **Koreańska Chmura Rządowa (GIDC)** - zamiast korzystać z publicznych chmur amerykańskiego czy chińskiego big tech'u, Korea Południowa zbudowała własną, silnie scentralizowaną infrastrukturę przetwarzania danych państwowych (*Government Integrated Data Center*). Opiera się ona na dwóch gigantycznych, superbezpiecznych centrach danych rządu w Daejeon i Gwangju. Administracja ma obowiązek korzystania w pierwszej kolejności z infrastruktury rozwijanej przez krajowe firmy.
- **Zabójcza dla big tech certyfikacja CSAP (Cloud Security Assurance Program)** - to najważniejsze narzędzie ochrony koreańskiego rynku chmurowego. Aby dostarczać usługi dla administracji publicznej, firma musi posiadać certyfikat CSAP. Przez lata wymagał on m.in. fizycznej separacji serwerów i sieci obsługujących sektor publiczny od tych dla sektora prywatnego. Dla globalnych graczy jak AWS, Google Cloud czy Microsoft Azure, których model biznesowy opiera się na współdzieleniu zasobów, było to nieopłacalne lub technicznie niemożliwe. W efekcie koreański rynek publiczny został w pełni zdominowany przez lokalnych graczy: Naver Cloud, KT Cloud i NHN Cloud. Ostatnio wprowadzono podział na poziomy bezpieczeństwa, ale najwyższe z nich nadal są de facto zarezerwowane dla lokalnych firm.
- **Sovereign AI (Narodowa Sztuczna Inteligencja)** - Korea odmawia oparcia swojej wiedzy, administracji czy wojska na rozwiązaniach zagranicznych (jak systemy OpenAI czy Google). Państwo przekierowuje potężne środki we współpracę rządu, ośrodków akademickich (np. KAIST) oraz koreańskich firm komercyjnych w celu stworzenia własnych, suwerennych dużych modeli językowych (LLM) oraz superkomputerów przeznaczonych wyłącznie do narodowych badań.
- **Suwerenność danych i twarde regulacje** - kraj ten prowadzi politykę twardego egzekwowania prawa wobec globalnych platform. Prawo w Korei rygorystycznie wymaga, aby wrażliwe dane obywateli i państwa były przechowywane fizycznie na serwerach zlokalizowanych w kraju. Nakłada to na zagranicznych dostawców usług chmurowych wymóg spełniania wyśrubowanych lokalnych standardów bezpieczeństwa i daje państwu ścisłą kontrolę nad transferem danych za granicę.
- **Dzielenie się niejawnymi danymi wojskowymi** - w dążeniu do dominacji w AI, w 2025 roku południowokoreański rząd wdrożył niezwykle odważny plan. Udostępnia on ściśle tajne dane wojskowe prywatnym firmom zbrojeniowym i technologicznym. Ma to na celu błyskawiczny rozwój zintegrowanych systemów bojowych kontrolowanych przez sztuczną inteligencję (takich jak autonomiczne roje dronów), co bezpośrednio przekłada się na bezpieczeństwo narodowe.

...

Korea Południowa

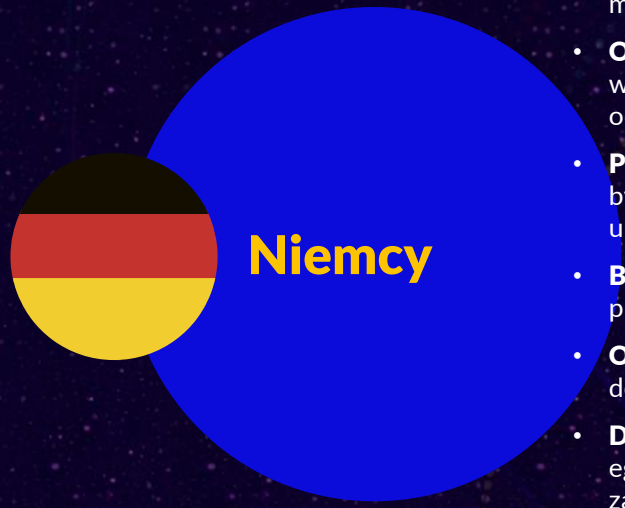
...

- **Dominacja w infrastrukturze (5G, 6G i Open Source)** - niezależność komunikacyjna jest kluczowa dla cyberbezpieczeństwa. Po sukcesie w masowym wdrożeniu sieci 5G, Korea już dziś oferuje miliardy dolarów w rozwój technologii 6G. Jednocześnie rząd bardzo mocno promuje wykorzystanie otwartego oprogramowania (open source) w sektorze publicznym, wspierając krajowy ekosystem twórców oprogramowania oraz rozwijając własne technologie kryptograficzne.
- **Krajowe algorytmy szyfrowania (KCMVP)** - w przetargach publicznych na oprogramowanie czy sprzęt sieciowy Korea Południowa rygorystycznie wymaga stosowania krajowych standardów kryptograficznych (np. algorytmów SEED lub ARIA), które muszą być certyfikowane przez Narodową Służbę Wywiadu (NIS) w ramach programu KCMVP. Zagraniczne firmy zazwyczaj stosują globalne standardy (np. AES) i rzadko decydują się na kosztowne przebudowywanie swoich produktów tylko pod wymogi koreańskiego wywiadu, co eliminuje je z przetargów.
- **System certyfikacji GS (Good Software) i NEP (New Excellent Product)** - państwo stworzyło specjalne krajowe certyfikaty jakości i innowacyjności. Zgodnie z prawem, koreańskie urzędy i agencje publiczne mają odgórny, procentowy obowiązek kupowania produktów posiadających te certyfikaty (np. nakaz przeznaczania co najmniej 20% budżetu na zakupy technologii z certyfikatem NEP). Ponieważ proces certyfikacji jest prowadzony w języku koreańskim, wymaga udostępniania kodów źródłowych i jest skrojony pod lokalny ekosystem, zagranicznym firmom niezwykle trudno go przejść. Dla koreańskich firm to z kolei darmowa „przepustka” do państwowych pieniędzy.



- **Kluczowe filary** - umowa koalicyjna rządu niemieckiego opiera suwerenność cyfrową na trzech głównych założeniach: suwerenności/niezależności, odporności (w tym cyber odporności) oraz interoperacyjności.
- **Wizja suwerennej Europy** - w Niemczech rośnie przekonanie, że suwerenność można osiągnąć wyłącznie w ramach zjednoczonej, współdziałającej Europy. Tylko na poziomie UE możliwa jest skala potrzebna do stworzenia konkurencyjnej infrastruktury cyfrowej.
- **Powołanie Federalnego Ministerstwa Cyfryzacji** - w 2025 roku Niemcy utworzyły odrębny, dedykowany resort koordynujący politykę cyfrową i modernizację rządu. Jest to centralny ośrodek decyzyjny, który zyskał realne narzędzia do narzucania standardów wszystkim szczeblom administracji – od rządu federalnego po samorządy.
- **Zukunftsfonds II** to niemiecki „fundusz funduszy" z 2025 roku o docelowym budżecie do 30 mld euro (min. 10 mld euro środków publicznych), który inwestuje wspólnie z rynkiem prywatnym (VC) w skalujące się europejskie spółki z sektora Deep Tech i biotechnologii, aby zatrzymać strategiczne innowacje na kontynencie i uniezależnić UE od globalnych gigantów.
- **Sovereign Tech Fund** to inicjatywa utworzona w 2022 roku przez niemieckie Ministerstwo Gospodarki (BMWK) w odpowiedzi na globalne luki w bezpieczeństwie oprogramowania, takie jak krytyczna podatność Log4j. Głównym celem funduszu jest budowa cyfrowej suwerenności i zmniejszenie zależności krajowej infrastruktury od zagranicznych gigantów technologicznych, takich jak Microsoft czy Amazon. Środki z funduszu przeznaczane są na finansowanie rozwoju, utrzymanie i zabezpieczanie kluczowych, otwartych technologii bazowych (open source), w tym bibliotek programistycznych, protokołów, narzędzi deweloperskich oraz technologii szyfrowania. Operacyjne zarządzanie całym przedsięwzięciem powierzono Sovereign Tech Agency, która jest wydzieloną spółką zależną od państwowej agencji innowacji SPRIND.
- **HighTech Agenda Deutschland** to ogłoszony w 2025 r. potężny program rządu federalnego i landów, którego celem jest uniezależnienie Niemiec od USA i Chin poprzez rozwój własnych kompetencji w krytycznych obszarach (m.in. AI, technologie kwantowe, biotechnologia i fuzja jądrowa). Jego absolutnym priorytetem jest **budowa suwerennego ekosystemu półprzewodników** – mimo niedawnego wycofania się amerykańskich inwestorów (Intel, Wolfspeed), plan zakłada budowę co najmniej trzech nowych fabryk (w tym zakładu Infineon w Dreźnie z publiczną dotacją 920 mln euro) oraz mocne wsparcie dla **Centrum Kompetencji Chip-Design** (zasilonego kwotą 50 mln euro), które we współpracy z instytutami Fraunhofera ma uniezależnić kraj w strategicznym procesie projektowania i prototypowania własnych układów scalonych.
- **Projekt „Deutschland-Stack" (D-Stack)** - najważniejsza nowość ogłoszona jesienią 2025 roku. Jest to narodowa, suwerenna platforma technologiczna dla sektora publicznego. Jej celem jest stworzenie otwartej, bezpiecznej i skalowalnej infrastruktury IT, która ułatwi współpracę na poziomie federalnym i przyśpieszy innowacje, oferując gotowe do użycia komponenty chmurowe i informatyczne.

...



- **Współpraca z rynkiem** - Niemcy nie budują D-Stacku w izolacji. W proces tworzenia włączono startupy, sektor MŚP, specjalistycznych dostawców IT oraz środowisko naukowe, aby platforma odpowiadała na realne zapotrzebowanie biznesowe i wspierała nowatorskie modele usług do 2028 roku (wtedy mają zostać oddane w pełni gotowe usługi dla administracji).
- **OpenCode i ocena zgodności** - niemiecki stack technologiczny w dużej mierze bazuje na platformie GitHub (OpenCode). Co więcej, wprowadzono centralny system oceny zgodności. Każdy standard i technologia ubiegająca się o wejście do D-Stack jest rygorystycznie oceniana w sześciu kategoriach pod kątem tego, czy realizuje cele cyfrowej suwerenności Niemiec (w tym kompatybilność europejską).
- **Promocja Open Source na poziomie ustawowym** - zgodnie z wytycznymi, standardy technologiczne na wszystkich szczeblach powinny być otwarte. Administracja federalna ma obowiązek preferowania oprogramowania open source tam, gdzie to tylko możliwe. Ma to na celu uniezależnienie państwa od zewnętrznych dostawców komercyjnych.
- **Bezpieczeństwo łańcuchów dostaw** - Niemcy stawiają na budowę zintegrowanych i bezpiecznych łańcuchów wartości obejmujących cały proces – od surowców aż po finalny sprzęt i oprogramowanie.
- **Ochrona infrastruktury krytycznej** - elementem niemieckiej cyber odporności jest systemowe wykluczanie tzw. „niegodnych zaufania dostawców" z możliwości dostarczania technologii dla infrastruktury krytycznej państwa.
- **Data Economy a prawo UE:** Rząd dąży do rozwoju gospodarki opartej na danych, podkreślając przy tym bezwzględną konieczność egzekwowania prawa cyfrowego UE (np. RODO czy DSA). Celem jest zabezpieczenie praw obywateli względem największych, zagranicznych platform cyfrowych.
- **Niemiecka Chmura Administracyjna (DVC)** to nowoczesna, wielochmurowa (multicloud) infrastruktura zaprojektowana dla administracji publicznej każdego szczebla, będąca efektem współpracy rządu federalnego, krajów związkowych i samorządów. DVC nie korzysta z usług amerykańskich gigantów, takich jak AWS, Google Cloud czy Microsoft Azure. Cała infrastruktura opiera się na otwartym oprogramowaniu i rygorystycznych, europejskich standardach ochrony danych. Głównym celem jest całkowite uniezależnienie państwa od pozaeuropejskich korporacji i wyeliminowanie ryzyka uzależnienia od jednego dostawcy (tzw. vendor lock-in).

O BADANIU OPINII PUBLICZNEJ

GŁÓWNY CEL BADANIA

Poznanie wiedzy i opinii Polaków na temat suwerenności technologicznej

METODOLOGIA

Badania online (CAWI) w ramach bloku pytań w Omnibusie GfK realizowane na GfK Access Panel
Długość wywiadu: ok. 7 minut

PRÓBA

Polacy w wieku 16-75 lat,
próba reprezentatywna ze względu na płeć, wiek, wykształcenie, miejsce zamieszkania
Liczebność próby: N=1000

TERMIN REALIZACJI

12-17.12.2025

Autorska definicja suwerenności technologicznej

Choć nie istnieje jedna, uniwersalna definicja suwerenności technologicznej, badacze realizujący niniejsze badanie CAWI wypracowali jej spójne ujęcie, które zostało przedstawione respondentom jeszcze przed przystąpieniem do właściwego przeprowadzenia badania. Definicję tę przygotowano na bazie gruntownej analizy dokumentów naukowych i analitycznych, ze szczególnym uwzględnieniem polskich opracowań. Należały do nich materiały stworzone dla Sieci Badawczej Łukasiewicz, takie jak „Indeks suwerenności technologicznej Polski" oraz „Cyfrowy Bilans Polski. Jak zmienić uzależnienie w suwerenność?", a także raporty CSM Think Tank („W dążeniu do suwerenności cyfrowej") i Polityki Insight („Techsuwerenność Europy. Od idei do praktyki"). Dodatkowo wspierano się dokumentami unijnymi takimi jak rozporządzenie UE 2024/795.

Aby dodatkowo zobrazować ten złożony koncept, w procesie tworzenia definicji badacze wykorzystali polskie i globalne narzędzia generatywnej sztucznej inteligencji (GenAI), w tym modele takie jak Bielik, Perplexity, Gemini oraz Deepseek. Pozwoliły one ukazać w ramach opracowanego pojęcia rolę kilku popularnych firm typu big tech z różnych krajów świata, które w praktyce stoją za kształtowaniem współczesnego rozumienia suwerenności technologicznej.

Definicja przedstawiana ankieterom

Suwerenność technologiczna oznacza zdolność firm, państwa (np. Polski) lub regionu (np. Unii Europejskiej) do samodzielnego rozwijania, wdrażania i kontrolowania kluczowych technologii w celu osiągnięcia niezależności, bezpieczeństwa i konkurencyjności na arenie międzynarodowej.

Ta zdolność obejmuje posiadanie własnych zasobów technologicznych, umiejętności badawczo-rozwojowych, infrastruktury produkcyjnej oraz odpowiedniego poziomu innowacyjności w strategicznych i krytycznych sektorach gospodarki (np. energetyce, zaopatrzeniu w wodę, sieciach telekomunikacyjnych).

Suwerenność technologiczna jako polityka państwa ma na celu wzmocnienie pozycji państw Unii Europejskiej w zakresie decyzji dotyczących technologii, uniknięcie zależności od innych krajów (np. Stanów Zjednoczonych, Korei Południowej czy Chin) lub podmiotów (np. Google, Microsoft, Amazon, Samsung czy Alibaba) oraz promowanie rozwoju gospodarczego i społecznego opartego na własnych osiągnięciach technologicznych.

PŁEĆ

49% 51%

WIEK

16-29	22
30-39	16
40-49	20
50-59	15
60-75	27

WYKSZTAŁCENIE

Podstawowe, niepełne podstawowe, gimnazjalne	16
Zasadnicze zawodowe lub średnie nieukończone	22
Średnie ukończone, pomaturalne, nieukończone wyższe	36
Licencjat, tytuł magistra, wyższe ukończone	26

MIEJSCE ZAMIESZKANIA

Wieś	40
Miasto do 49 tys.	24
Miasto od 50 do 500 tys.	24
Powyżej 500 tys.	12

GENERACJA

Gen Z (16-28 lat)	19
Gen Y (29-44 lat)	29
Gex X (45-60 lat)	27
Baby boomers (61+)	25

WIELKOŚĆ GOSPODARSTWA DOMOWEGO

1 osoba	23
2 osoby	25
3 osoby	19
4 osoby	16
5 lub więcej osób	17

MIESIĘCZNE DOCHODY NETTO GOSPODARSTWA DOMOWEGO

do 4499 PLN	23
4500 - 6999 PLN	18
7000 - 9999 PLN	16
10.000 PLN i więcej	26
Odmowa podania	18

W wyniku zaokrągleń wskazania sumują się do 101%

AUTORZY I EKSPERCI PUBLIKACJI

Piotr Mieczkowski

Dyrektor zarządzający i członek zarządu fundacji Digital Poland, wiceprezes zarządu European AI Forum, członek zarządu KIGEiT, przewodniczący AI Poland, wiceprzewodniczący TechPL, wiceprzewodniczący Komisji ds. Cyfryzacji w Mieście Warszawa, członek grup, zespołów i przewodniczący przy Ministerstwie Cyfryzacji, wykładowca Akademii Leona Koźmińskiego, członek rady biznesowej Bielik.AI

Piotr ma ponad 20-letnie doświadczenie w realizacji projektów w sektorze nowych technologii. Obecnie zarządza pracami fundacji Digital Poland, która promuje cyfryzację jako element przewagi konkurencyjnej Polski. Jest członkiem zarządu najstarszej i najbardziej reprezentatywnej Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji z obszaru ICT, która skupia takie inicjatywy jak AI Poland, GameDev Poland czy TechPL. Piotr jest również wiceprezesem zarządu European AI Forum – największej organizacji europejskich spółek AI z siedzibą w Brukseli, które gromadzi ponad 3000 startupów AI z 14 europejskich krajów. Piotr jako wiceprzewodniczący aktywnie uczestniczy w BKDS ds. Cyfryzacji przy Urzędzie m. st. Warszawa, Zespole ds. wsparcia polskiego sektora ICT jako przewodniczący internacjonalizacji i marki polskiej przy Ministerstwie Cyfryzacji, jest członkiem Komitetu Monitorującego FENG z ramienia Federacji Przedsiębiorców Polskich i członkiem grup roboczych przy Ministerstwie Cyfryzacji. Piotr dzieli się również wiedzą np. na studiach podyplomowych na Akademii Leona Koźmińskiego z zakresu sztucznej inteligencji.

Piotr jest autorem lub współautorem wielu raportów, publikacji, artykułów oraz polityk publicznych wspierających sektor nowych technologii, w tym sztucznej inteligencji (AI), internetu rzeczy (IoT), cyberbezpieczeństwa czy sieci 5G. Piotr jest współtwórcą strategicznego programu NCBR AI INFOSTRATEG, który wspiera wdrożenie AI w Polsce kwotą 840 mln zł. Aktywnie współtworzył też szereg polityk sektorowych i głównych strategii w Polsce.

Piotr posiada praktyczne doświadczenie w zakresie transformacji cyfrowej, tworzenia skutecznych polityk publicznych opartych na danych, procesów biznesowych, tworzenia programów edukacyjnych, doradztwa strategicznego czy projektowania rozwiązań ICT. Posiada aktualną wiedzę na temat takich zagadnień jak sztuczna inteligencja, duże zbiory danych, przetwarzanie w chmurze, internet rzeczy, sieci 5G czy inteligentne miasta.

Piotr pracował wcześniej w globalnej firmie doradczej (EY), w zintegrowanej grupie medialno-telekomunikacyjnej (Grupa Polsat Plus), operatorze sieci komórkowej (Orange) oraz w globalnej firmie energetycznej (Shell). Zrealizował z sukcesem ponad 37 projektów dla takich klientów jak Deutsche Telekom, E&, Liberty Global, Multimedia Polska, Netia, Orange, Telenor, T-Mobile, Saudi Telekom Company, Solutions by STC, UPC, Vodafone. Piotr pracował również dla regulatorów w regionie CEE, np. UKE, NMHH, GNCC, SPRK, RRT oraz kluczowych decydentów, np. Ministerstwa Cyfryzacji w Polsce, izb branżowych np. KIGEiT, PIIT czy agencji grantowych np. NCBR. Realizował również projekty doradcze m. in. we współpracy Artur D. Little, BCG czy EY-Parthenon.

Jest absolwentem Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej oraz Wydziału Zarządzania Uniwersytetu Warszawskiego. Posiada szereg specjalistycznych certyfikatów technicznych i menedżerskich.

W swoich działaniach skupia się na współpracy, budowaniu aktywnych społeczności i przede wszystkim na wypracowywaniu konkretnych wyników na bazie faktów i danych, a nie emocji czy przekonań.

AUTORZY I EKSPERCI PUBLIKACJI

dr Michał Boni
Fundacja Digital Poland

Cristina Caffarra
EuroStack Initiative Foundation

Maciej Kuźniar
Oktawave

Bartosz Łopiński
Billennium

Marcin Madey
SUSE Polska

Wiesław Wilk
Związek Polska Chmura

Maciej Wyczesany
Apator S.A.

Krzysztof Pstrong
Polska Izba Komunikacji Elektronicznej (PIKE)

O FUNDACJI DIGITAL POLAND
I DIGITAL FESTIVAL 2025

digitalpoland

O Fundacji Digital Poland

Jako organizacja non-profit, Fundacja podejmuje działania na rzecz tego, aby Polska stała się jednym z wiodących światowych centrów innowacji cyfrowych. Naszą wizją jest przyspieszenie cyfryzacji kraju tak, aby społeczeństwo, przedsiębiorstwa i instytucje publiczne potrafiły w pełni wykorzystywać technologie w sposób mądry, świadomy i odpowiedzialny.

Fundacja zamienia stojące przed Polską wyzwania cyfrowe w realne szanse dla krajowej gospodarki. Jesteśmy przekonani, że bez aktywnego udziału obywateli rozwój technologiczny nie będzie możliwy. Dlatego stawiamy na edukację – organizujemy liczne wydarzenia i akcje edukacyjne, takie jak Digital Fitness Test, Digital Ars, Akademia SkillUp, Digital Festival czy Noc Innowacji, które popularyzują nowe technologie w życiu codziennym i biznesie.

Na arenie międzynarodowej prezentujemy Polskę jako atrakcyjne miejsce do prowadzenia działalności badawczo-rozwojowej i tworzenia innowacji o globalnym zasięgu, wykorzystując wiedzę i kompetencje polskich specjalistów ICT. Pomagamy też skalować biznes promując krajowe rozwiązania na wiodących konferencjach takich jak Web Summit, Vivatech, London Techweek czy organizując wizyty studyjne co światowych centrów innowacji.

Prowadzimy także szeroko zakrojone analizy spraw publicznych. Współtworzymy największy w Polsce zestaw rekomendacji – „Czas na cyfrową gospodarkę" – wyznaczający kierunki rozwoju innowacji i strategicznego myślenia o roli cyfryzacji w społeczeństwie i gospodarce. Regularnie realizujemy badania konsumentów i przedsiębiorstw, publikując bezpłatne raporty, m.in. dotyczące dezinformacji, sztucznej inteligencji czy największych firm technologicznych. Organizujemy również debaty publiczne na temat wpływu technologii na życie społeczne i biznesowe.

Fundacja jest jednym z założycieli European AI Forum w Brukseli – największej w Europie organizacji zrzeszającej ponad 3000 startupów AI (więcej na eaiforum.org). Zainicjowała również wiodące krajowe przedsięwzięcia, takie jak AI Poland czy TechPL, działające przy Krajowej Izbie Gospodarczej Elektroniki i Telekomunikacji (więcej na kigeit.org.pl).

We wszystkich naszych działaniach stawiamy na współpracę i budowanie sieci partnerskich relacji. Wierzymy, że tylko dzięki otwartości i wspólnym inicjatywom możemy uczynić Polskę jednym z globalnych liderów innowacji cyfrowych.

Zapraszamy do współpracy wszystkich, którzy chcą realizować projekty edukacyjne, innowacyjne oraz związane z politykami publicznymi – projekty, które pozytywnie zmieniają polską gospodarkę. Wśród fundatorów i partnerów strategicznych Fundacji są m.in.: Baker McKenzie, Fujitsu, Polpharma, Ringier Axel Springer Polska, Symfonia, T-Mobile Polska, TVN Warner Bros. Discovery, Visa, a w gronie partnerów znajdują się także takie firmy, jak Prowly czy Techland.

Chcesz dowiedzieć się więcej? Odwiedź digitalpoland.org

STRATEGICZNI FUNDATORZY I STRATEGICZNI PARTNERZY

PARTNERZY

digitalpoland

Międzybranżowa, ogólnokrajowa inicjatywa skupiająca się na wynikach naszych działań

Współdzielimy i prowadzimy inicjatywy i koalicje cyfrowe, współpracujemy, tworzymy sieć kontaktów i promujemy cyfryzację w wiodących mediach

Pomagamy przekształcać cyfrowe wyzwania w szanse dla polskiej gospodarki i społeczeństwa poprzez tworzenie najlepszych polityk cyfrowych

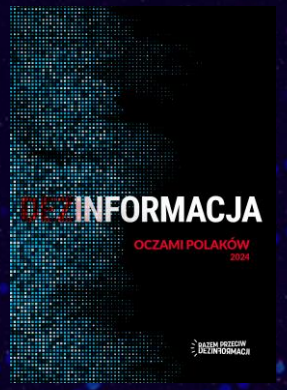
Promujemy Polskę jako wiodący ośrodek innowacji cyfrowych

Edukujemy społeczeństwo, prezentujemy fakty, obalamy mity, podpowiadamy jak korzystać z nowych technologii

Mamy udokumentowane osiągnięcia. Przykłady naszych inicjatyw.

- Digital Festival
- Digital Shapers
- Polityki cyfrowe
- Czas na cyfrową gospodarkę
- AI Hub
- European AI Forum
- Koalicja „Cyfrowi Seniorzy”
- Think Tank
- Study Tours
- Koalicja „Razem przeciw dezinformacji”
- Digital CEO
- Digital Champions CEE
- Digital Fitness Test
- Digital Summit
- Polska jako centrum R&D
- Akademia SkillUp

Wspólnie z partnerami prowadzimy działalność edukacyjną i badawczą. Jesteśmy niezależnym think-tankiem. Pobierz bezpłatnie wszystkie nasze materiały ze strony fundacji po uprzedniej rejestracji.



Digital Festival _2025

Zobacz jak było w 2025 r.

6
tygodni
edukacji o AI

200+
partnerów

130+
wydarzeń
online/offline

dotarliśmy do
11+ mln
osób w mediach
ogólnopolskich

dotarliśmy do
4,6+ mln
osób w mediach
społecznościowych

Nowoczesny Senior

rozesłaliśmy
13,6 tys.
poradników „Nowoczesny senior”
online oraz drukowanych

30+ tys.
przeszkolonych seniorów

52,3 mln
zasięg informacji

Digital Fitness Test

11,2+ tys.
osób wykonało quiz

Noc Innowacji

16
miast

100+
wydarzeń

11,7+ tys.
uczestników

112,5 mln
zasięg informacji

Strefa wiedzy

15+
wideopodcastów

20
artykułów o AI

Akademia SkillUp

90+
szkoleń

SUWERENNOŚĆ TECHNOLOGICZNA POLSKI I EUROPY

Raport z badania opinii społecznej. Edycja 2026.

digitalpoland