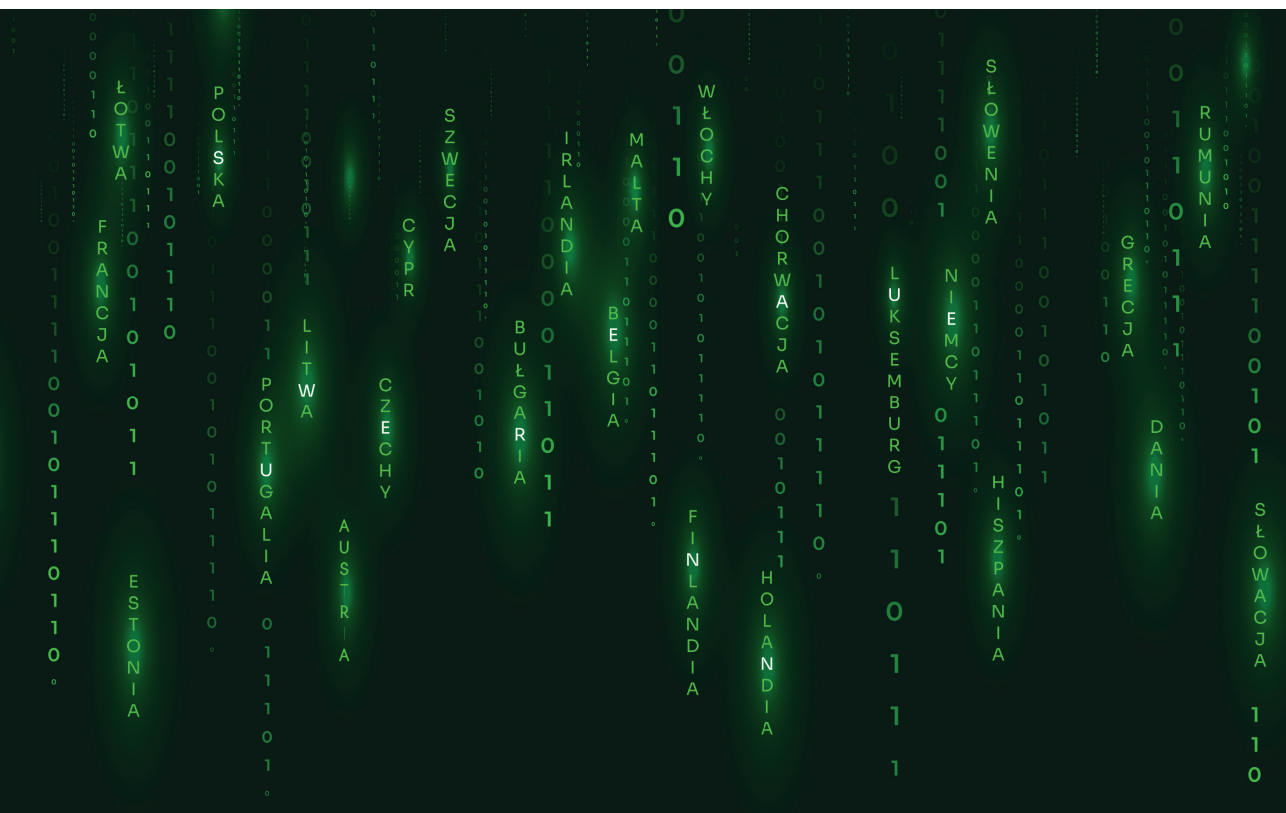




**Reforma Cyfrowej dekady. Jak
uwzględnić suwerenność
technologiczną w kluczowej
strategii cyfrowej UE?**

Cytowanie: Święcicki, I., Witczak, J. (2025), Reforma Cyfrowej dekady. *Jak uwzględnić suwerenność technologiczną w kluczowej strategii cyfrowej UE?*, Policy Paper, nr 6, Polski Instytut Ekonomiczny, Warszawa.

Policy Paper 6/2025

Warszawa, listopad 2025 r.

Autorzy: Ignacy Święcicki, Jakub Witczak

Redakcja merytoryczna: Paweł Śliwowski

Redakcja: Jakub Nowak, Małgorzata Wieteska

Projekt graficzny: Anna Olczak

Skład i łamanie: Tomasz Gałązka

Polski Instytut Ekonomiczny

Al. Jerozolimskie 87

02-001 Warszawa

© Copyright by Polski Instytut Ekonomiczny

Spis treści

Kluczowe wnioski	4
Wprowadzenie	6
Propozycje wskaźników powiązanych z suwerennością	8
Wykorzystanie koncepcji stosu technologicznego do oceny poziomu suwerenności technologicznej	8
Cyfrowe usługi publiczne	10
Umiejętności cyfrowe	14
Modyfikacje pozostałych wskaźników	
Cyfrowej dekady	16
Infrastruktura cyfrowa	16
Cyfrowa transformacja biznesu	18
Cyberbezpieczeństwo	21
Bibliografia	24

Kluczowe wnioski

- Niniejszy policy paper stanowi wkład do planowanego na 2026 r. przeglądu Cyfrowej dekady – programu polityki mającej zapewnić transformację cyfrową, podnieść konkurencyjność i odbudować suwerenność technologiczną w Unii Europejskiej. Mimo odniesienia do kwestii suwerenności cyfrowej w Decyzji ustanawiającej program polityki „Droga ku cyfrowej dekadzie” do 2030 r. (motyw 1 Decyzji 2022/2481), **przyjęte wskaźniki realizacji celów nie odnoszą się do tego celu w wystarczający sposób. Przygotowaliśmy 12 rekomendacji dotyczących obszarów, celów i wskaźników, które powinny zostać uwzględnione w przyszłorocznych pracach.**
- **Najważniejszym elementem naszej propozycji jest zintegrowanie celów i wskaźników Cyfrowej dekady z wybranymi celami polityki przemysłowej UE służącej wzmocnieniu europejskiej suwerenności technologicznej.** Temu poświęciliśmy pięć pierwszych rekomendacji.
- Przede wszystkim zalecamy wykorzystanie **konceptu stosu technologicznego** do mierzenia suwerenności oraz wskazanie konkretnego poziomu suwerenności w poszczególnych warstwach stosu (np. półprzewodniki, chmura obliczeniowa, oprogramowanie). **Celem może być zwiększenie europejskiego udziału w rynku w danej warstwie stosu** (np. dwukrotnie – podobnie jak to jest obecnie sformułowane w przypadku półprzewodników) **lub ograniczenie ryzykownych zależności** (np. odsetek usług lub produktów pochodzących od jednego dostawcy czy z jednego państwa) (-> rekomendacja 1).
- W obszarze usług publicznych proponujemy skupienie się na ochronie zdrowia i dążenie **do zwiększenia suwerenności w zakresie przechowywania i przetwarzania danych medycznych** Europejczyków. Mogą do tego zostać wykorzystane istniejące wytyczne KE dotyczące chmury obliczeniowej. Obszar ochrony zdrowia jest również ważny dla Polski – obie polskie fabryki AI wskazały go jako priorytetowy (-> rekomendacja 2).
- Zalecamy przejście od oceny dostępności danych medycznych do uruchomienia konkretnych rozwiązań wykorzystujących te dane. Nasza propozycja zakłada **uruchomienie narzędzi predykcyjnych dla określonej liczby jednostek chorobowych** (przy zachowaniu zasady suwerenności na poziomie danych i modeli) pozwalających na poprawę profilaktyki zdrowotnej i wczesnego ostrzegania przed poważnymi zachorowaniami (-> rekomendacja 3, zgodna z polską Strategią cyfryzacji państwa).
- W kluczowym dla długofalowego rozwoju **obszarze edukacji i kompetencji cyfrowych sugerujemy uruchomienie publicznego wsparcia certyfikacji umiejętności wykorzystania otwartoźródłowych systemów IT.** Program taki mógłby obejmować finansowanie kursów zakończonych certyfikacją w szkołach średnich i wyższych oraz późniejszej akceptacji takich certyfikatów przez pracodawców z sektora publicznego, w celu ugruntowania ich wykorzystania (-> rekomendacja 5) (Klekowski, 2025).

- Ostatnią rekomendacją nawiązującą bezpośrednio do kwestii suwerenności cyfrowej jest wprowadzenie pomiaru suwerenności cyfrowej na poziomie lokalnym – w jednostkach samorządu terytorialnego, jednostkach edukacyjnych czy opieki zdrowotnej (-> rekomendacja 4). Ten obszar instytucjonalny nie jest objęty systematycznym monitoringiem, a jego rola wydaje się niezwykle istotna, zarówno w zakresie wrażliwości na ewentualne zakłócenia, jak i wspieranie rozwiązań krajowych lub europejskich.
- Oprócz włączenia kwestii suwerenności cyfrowej, **proponujemy również zmiany w innych celach**, wynikające albo z faktu, że dotychczasowe się wyczerpują (np. są bliskie osiągnięcia celu i perspektywa 2035 r. wymaga postawienia nowych celów) albo z konieczności dopasowania ich do zmieniających się polityk unijnych.
- Modyfikacje celów i wskaźników w zakresie **łączności** obejmują skupienie się na głównych szlakach transportowych (-> rekomendacja 6, cel wskazywany już w komunikacie „W stronę społeczeństwa gigabitowego”, jednak wciąż nieosiągnięty), a także odejście od kosztownego i niemożliwego do zrealizowania celu dotarcia do wszystkich gospodarstw domowych z siecią przewodową w technologii światłowodowej (-> rekomendacja 7).
- W zakresie **cyfrowej transformacji firm** proponowane przez nas wskaźniki mają być wykorzystywane do pomiaru realnych efektów działań w zakresie wsparcia innowacyjnych firm. Przykładowo, problemem Europy jest ucieczka młodych i rosnących firm za ocean, a nie sam brak obiecujących start-upów, dlatego **należy zwrócić uwagę na to, gdzie dokonuje się tzw. exit** (-> rekomendacja 8). Istniejący dystans firm europejskich od liderów innowacji cyfrowych można mierzyć wydatkami na badania i rozwój w grupie firm z branży cyfrowej (-> rekomendacja 9). Dodatkowo proponujemy objęcie badaniami mikrofirm stanowiących większość (liczbowo) w gospodarce europejskiej (-> rekomendacja 10).
- Proponujemy rozszerzenie Cyfrowej dekady o cele i wskaźniki z obszaru cyberbezpieczeństwa, niezwykle ważnego obszaru, choć nieobecne-go dotychczas w tym programie. W tym wypadku można wykorzystać istniejące miary opracowane przez ENISA (2025) (-> rekomendacja 12). Bazując na polskich doświadczeniach z programu Cyberbezpieczny samorząd proponujemy również objęcie samorządów oceną poziomu cyberbezpieczeństwa.

Wprowadzenie

Trwa przegląd programu „Droga ku cyfrowej dekadzie”, który wyznacza cele transformacji cyfrowej UE do 2030 r. Przegląd wynika nie tylko z formalnych wymogów¹, lecz także ze zmian zachodzących w politykach publicznych w obszarze cyfryzacji. Nowy skład Komisji Europejskiej i na nowo sformułowane obszary pracy i misja Kolegium Komisarzy prowadzą w naturalny sposób do przeglądu przyjętych wcześniej kierunków rozwoju. Jednocześnie coraz większa presja na wzmacnianie europejskiej suwerenności technologicznej i cyfrowej wymusza aktualizację celów i wybór nowych wskaźników stosowanych do pomiaru ich realizacji.

Mimo odniesienia do kwestii suwerenności cyfrowej w Decyzji ustanawiającej program polityki „Droga ku cyfrowej dekadzie” do 2030 r. (motyw 1 Decyzji 2022/2481), przyjęte wskaźniki realizacji celów nie odnoszą się do tego celu w wystarczający sposób. Skala zależności państw Unii Europejskiej od zewnętrznych dostawców usług chmurowych, podkreślana m.in. w raporcie Draghiego (2024) czy zależności w kilku warstwach tzw. stosu technologicznego (Bria, Timmers, Gernone, 2025), prowadzi do wniosku, że same mierniki poziomu cyfryzacji firm, kompetencji cyfrowych, rozwoju start-upów czy wreszcie ucyfrowienia administracji publicznej nie są wystarczające. Skupienie na tego typu miernikach² może prowadzić do utrzymania lub pogłębienia zależności cyfrowych i utrzymania słabej pozycji Unii Europejskiej w światowej gospodarce cyfrowej. W naszej ocenie jedynym obecnie wykorzystywanym wskaźnikiem, który jest bezpośrednio związany z odbudową suwerenności, jest udział UE w globalnym rynku półprzewodników.

Z powyższych powodów proponujemy konkretne zmiany w celach Cyfrowej dekady i wskaźnikach jej mierzących. Należy przy tym podkreślić, że taka zmiana wskaźników jest naturalna w tego typu wieloletnich strategiach – wynika z wyczerpania się niektórych miar (np. bliskość osiągnięcia zakładanego celu), zmian w zakresie polityk publicznych (coraz większe znaczenie wspomnianej kwestii suwerenności) czy konieczności uwzględnienia nowych obszarów.

¹ Art. 4 ust. 2 Decyzji Parlamentu Europejskiego i Rady (UE) 2022/2481.

² Pełny opis mierników cyfrowej dekady, jednak bez odniesienia do problematyki suwerenności cyfrowej został przedstawiony w opracowaniu Świącieckiego i Witczaka (2023).

Punktem wyjścia jest dla nas ostatni raport o stanie Cyfrowej dekady (Komisja Europejska, 2025a), przedstawiający stopień realizacji wszystkich dotychczasowych celów. W niniejszym opracowaniu nie prowadzimy zatem systematycznej oceny punktu, w którym się znajdujemy. Jednocześnie odnosimy się do polskiej specyfiki i krajowych strategii z obszaru cyfrowego: Strategia cyfryzacji państwa (Ministerstwo Cyfryzacji, 2025a), Polityka rozwoju sztucznej inteligencji (Ministerstwo Cyfryzacji, 2025b), Polityka dla sektora półprzewodników (Ministerstwo Cyfryzacji, 2025c) i wskażemy – na ile to możliwe – znaczenie proponowanych zmian z polskiego punktu widzenia i ich powiązania z przyjętymi bądź konsultowanymi dokumentami. Wreszcie, staramy się odnieść do innych działań realizowanych na poziomie UE, osadzając nasze propozycje w szerokim nurcie polityk publicznych UE, podkreślając powiązania między obszarami i przekrojowe znaczenie transformacji cyfrowej.

Propozycje wskaźników powiązanych z suwerennością

Wykorzystanie koncepcji stosu technologicznego do oceny poziomu suwerenności technologicznej

W dyskusji o wbudowaniu działań na rzecz wzmacniania suwerenności technologicznej w ramy Cyfrowej dekady warto oprzeć się na koncepcji stosu technologicznego (Bria, Timmers, Gernone, 2025). Tego typu opis zależności i powiązań między podstawowymi produktami (półprzewodniki), usługami (chmura), infrastrukturą (sieci, centra danych), platformami i aplikacjami pozwala na określenie poziomu zależności oraz monitorowanie efektów podejmowanych działań. **Wskazuje się, że 80 proc. rynku chmury obliczeniowej w UE jest obsługiwane przez firmy spoza Europy (Draghi, 2024), a zależność od podaży urządzeń mobilnych jest niemal stuprocentowa.** Obecnie w ramach Cyfrowej dekady monitorowany jest udział podmiotów z Unii Europejskiej w globalnym rynku półprzewodników (obecnie wynosi 10,5 proc., cel to 20 proc.) (Komisja Europejska, 2025a). Brakuje obecnie powszechnie uznanych miar suwerenności technologicznej. Jak wskazują Święcicki i Witczak (2025b), Komisja Europejska ma wypracowaną metodologię szacowania zależności w handlu towarami (Garcia, Ho, 2025), przydatną np. do zależności w obszarze półprzewodników czy sprzętu sieciowego, jednak trudniejsze jest precyzyjne wskazanie poziomu zależności (czy też będącej jej odwrotnością suwerenności) w warstwach, na które składają się usługi.

REKOMENDACJA 1.

Wykorzystanie koncepcji stosu technologicznego do mierzenia suwerenności oraz wskazanie konkretnego poziomu suwerenności w poszczególnych warstwach stosu (np. półprzewodniki, chmura obliczeniowa, oprogramowanie). Celem może być zwiększenie europejskiego udziału w rynku w danej warstwie stosu (np. dwukrotnie – podobnie jak to jest obecnie sformułowane w przypadku półprzewodników) lub ograniczenie ryzykownych zależności (np. odsetek usług/productów pochodzących od jednego dostawcy czy z jednego państwa).

Operacjonalizacja

Dla szacowania obecnego poziomu zależności w warstwie półprzewodników, surowców czy urządzeń można wykorzystać istniejącą metodologię EXVI i prowadzone już szacunki przez JRC (Bonnet, Ciani, 2023). W przypadku pozostałych warstw w początkowym etapie można posiłkować się danymi rynkowymi (np. udział w rynku chmury obliczeniowej), danymi handlowymi (zwracając uwagę na ich ograniczenia – znacznie mniejsza szczegółowość niż w przypadku danych dla handlu towarami). Można wykorzystać istniejące wskaźniki, takie jak Digital Dependence Index lub uznane miary, jak np. wskaźnik Herfindahla-Hirschmana dla mierzenia koncentracji w imporcie. Dla określenia krytycznych poziomów zależności i określenia poziomów docelowych można odnieść się do wskazań przyjętych w akcie o surowcach krytycznych (Rozporządzenie PE i Rady UE 2024/1252) – jednym z celów jest ograniczenie zależności od jednego kraju dostawcy do nie więcej niż 65 proc. podaży danego surowca.

W dłuższym okresie konieczne może się okazać wypracowanie odrębnej metodologii szacowania zależności w handlu usługami, w tym uzyskanie bardziej szczegółowych danych handlowych.

Znaczenie dla Polski

Suwerenność pojawia się w wielu miejscach powstającej strategii cyfryzacji państwa – w zakresie cyberbezpieczeństwa, chmury obliczeniowej, danych czy zamówień publicznych. Polska nie posiada obecnie zdefiniowanych poziomów zależności w poszczególnych warstwach stosu technologicznego, jednak istniejące i powstające strategie sektorowe, np. Polityka dla sektora półprzewodników (Ministerstwo Cyfryzacji, 2025c), Polityka rozwoju sztucznej inteligencji (Ministerstwo Cyfryzacji, 2025b) mają na celu budowę polskich zdolności produkcyjnych w sektorach odpowiadających poszczególnym warstwom stosu technologicznego. Przyjęcie tego typu podejścia i wskaźników na poziomie UE będzie mogło wesprzeć krajowe działania w tym zakresie.

Powiązanie z innymi politykami UE

Suwerenność technologiczna jest obecnie jednym z głównych wątków dyskusji o polityce przemysłowej i bezpieczeństwie w Unii Europejskiej. Na znaczenie tematu wskazuje m.in. desygnowanie wiceprzewodniczącej Komisji Europejskiej, której zakres obowiązków obejmuje właśnie suwerenność technologiczną, a także obecność tego wątku w przemówieniach oficjeli KE i przedstawicieli państw członkowskich. Na kwestię wzmacniania niezależności wskazuje też Mario Draghi (2024). Podobny problem ma być rozwiązywany przy pomocy wspomnianego aktu o surowcach krytycznych, a w jednym z niedawnych postępowań w ramach zamówień publicznych na zakup usług chmury obliczeniowej po raz pierwszy Komisja Europejska przedstawiła katalog kryteriów oceny poziomu suwerenności zamawianych usług.

Cyfrowe usługi publiczne

Praktyczne działania na rzecz odbudowy suwerenności cyfrowej mogą być realizowane przy tworzeniu cyfrowych usług publicznych. To tu decyzje mają najbardziej bezpośredni wpływ na decyzje dotyczące rozwiązań technologicznych.

Dbałość o kontrolę nad danymi, strategię unikania zależności w kluczowych procesach czy wspieranie rozwoju europejskiego ekosystemu technologicznego to działania, które mogą stanowić przykład dla sektora prywatnego i poszerzać zrozumienie dla korzyści płynących z oparcia się na rozwiązaniach suwerennych. Jednocześnie warto zwrócić uwagę, że **wskaźniki mierzące cele w filarze cyfrowych usług publicznych są obecnie na wysokim poziomie realizacji i przekraczają 80 proc. zamierzonych celów**. W takiej sytuacji warto rozważyć przejście od bardziej ogólnych miar, dotyczących działań administracji centralnej, do bardziej szczegółowych celów cyfryzacji państw członkowskich. W ramach takiego pogłębienia można skupić się na specyficznych celach sektorowych oraz zejściu na niższy szczebel administracyjny, np. samorządów. **Administracja na poziomie samorządów pozostaje często mniej zaawansowana cyfrowo, ale także bardziej wrażliwa na zaburzenia w dostępie i funkcjonowaniu technologii, mają bowiem ograniczone zasoby do szybkiego reagowania na pojawiające się problemy**.

Wśród obecnych celów Cyfrowej dekady jest zapewnienie pełnego dostępu do elektronicznych danych medycznych dla obywateli. Cel jest obecnie bliski realizacji (82,7 proc. wartości docelowej), jednak należy monitorować jego realizację w założonym pierwotnie terminie – do 2030 r. W perspektywie 2035 r. warto natomiast wyznaczyć nowe cele, odpowiadające rosnącym europejskim ambicjom w sferze bezpieczeństwa i zapewniania suwerenności. Przy tym podejściu dotychczasowy cel mógłby mieć charakter wskaźnika technicznego, który w przyszłości zostałby wygaszony (po oczekiwanym osiągnięciu poziomu 100 proc.).

Rekomendujemy podjęcie działań w kierunku sprawowania pełniejszego nadzoru nad danymi przechowywanymi w systemie ochrony zdrowia przez wykorzystanie wytycznych Komisji Europejskiej do określania poziomu suwerenności chmury obliczeniowej (Komisja Europejska, 2025b). Wytyczne te uwzględniają dobre praktyki stosowane w państwach członkowskich UE, występowanie zagrożeń w międzynarodowym handlu towarami i usługami oraz potrzebę weryfikacji zabezpieczeń deklarowanych przez dostawców usług chmurowych. W kontekście danych tak wrażliwych, jak dane medyczne, warto rozważyć wprowadzenie wytycznych dążących do zwiększenia suwerenności powiązanej z nimi infrastruktury chmurowej, zgodnie z wytycznymi KE. Takie działanie byłoby także elementem podnoszenia świadomości wśród państw członkowskich co do tego, że infrastruktura nie jest neutralna, a decyzje z nią związane powinny uwzględniać aspekt sprawowania nadzoru.

REKOMENDACJA 2.

Dążenie do zwiększenia suwerenności w zakresie przechowywania i przetwarzania danych medycznych Europejczyków poprzez wprowadzenie metodologii oceny poziomu suwerenności infrastruktury chmurowy obliczeniowej w obszarze zdrowia i osiągnięcie wysokiego poziomu suwerenności (np. zgodnie z wytycznymi Komisji Europejskiej (2025b) na poziomie SEAL3³ lub wyższym).

Operacjonalizacja

Raportowanie na poziomie państw członkowskich UE odsetka systemów chmurowych wykorzystywanych w publicznych systemach ochrony zdrowia wykorzystywanych do przetwarzania danych medycznych zgodnych z wytycznymi KE na poziomie SEAL3 lub wyższym.

Dodatkowo, w ramach pogłębiania celów w zakresie ochrony zdrowia, warto zauważyć, że obecny cel (100 proc. obywateli posiada elektroniczny dostęp do swoich danych medycznych) może zostać osiągnięty już w 2027 r. (Komisja Europejska, 2025c). Racjonalne wydaje się zatem pójście o krok dalej i skupienie się na konkretnych efektach transformacji cyfrowej sektora ochrony zdrowia. Takim efektem może być wzmocnienie profilaktyki zdrowotnej – wykorzystanie danych medycznych i algorytmów sztucznej inteligencji do poprawy jakości zdrowia obywateli i obniżenia kosztów opieki zdrowotnej.

REKOMENDACJA 3.

Zmiana celu w zakresie cyfrowych usług zdrowotnych – odejście od mierzenia dostępności danych medycznych (lub pozostawienie jako miary technicznej, z terminem realizacji 2030 r.) i wprowadzenie celu na 2035 r. w postaci uruchomienia narzędzi predykcyjnych (dla określonej liczby jednostek chorobowych, przy zachowaniu zasady suwerenności na poziomie danych i modeli) pozwalających na poprawę profilaktyki zdrowotnej i wczesnego ostrzegania przed poważnymi zachorowaniami.

Operacjonalizacja

Celem mogłaby być liczba jednostek chorobowych, dla których wprowadzono narzędzia predykcyjne w systemie ochrony zdrowia (np. 100 do 2035 r.). Obecnie brakuje danych tego typu, zaś ich zebranie wymagałoby dodatkowego badania, a także wykorzystania standardów określających poziomy suwerenności rozwiązań IT.

³ Poziom suwerenności chmurowej SEAL3 wg wytycznych Komisji Europejskiej oznacza, że prawo UE ma zastosowanie i jest egzekwowane, podmioty UE wywierają znaczący, ale niepełny wpływ; usługi, technologie lub operacje podlegają marginalnej kontroli stron trzecich spoza UE.

Znaczenie rekomendacji 2 i 3 dla Polski

Rozbudowa europejskiej suwerenności cyfrowej w zakresie zdrowia jest spójne z polskimi ambicjami, których wyrazem są specjalizacje polskich fabryk AI. **Zarówno poznańska fabryka PIAST-AI, jak i krakowska Gaia AI Factory mają w swoich celach zastosowanie mocy obliczeniowych do celów ochrony zdrowia i medycyny.** Dodatkowo przygotowywana Strategia cyfryzacji państwa zakłada jako jeden z celów wprowadzenie narzędzi predykcyjnych w systemie centralnym.

Powiązanie z innymi politykami UE

Jest zgodne z założeniami rozporządzenia o Europejskiej Przestrzeni Danych Medycznych (EHDS), które kładzie nacisk na bezpieczeństwo danych medycznych oraz spójne z wytycznymi NIS2 o bezpieczeństwie łańcucha dostaw. Wykorzystanie narzędzi predykcyjnych w systemach opieki zdrowotnej pozwoli na praktyczne wykorzystanie danych medycznych gromadzonych w ramach EHDS, będzie też dodatkową motywacją do cyfryzacji jednostek medycznych.

Budowa europejskiej suwerenności cyfrowej wymaga w dużej mierze zrozumienia istniejących zależności. Dopiero wtedy możliwa będzie ocena ryzyk, jakie wynikają z zależności oraz projektowanie działań, mających na celu ich minimalizowanie. Możliwym działaniem jest wprowadzenie regularnych sprawozdań jednostek samorządu terytorialnego oraz podmiotów im podległych pod kątem występowania zależności cyfrowych. Sprawozdania mogą odbywać się w ramach samooceny na podstawie jednolitych ram umożliwiających ocenę występujących zależności cyfrowych w obszarach takich jak: systemy informatyczne (ocena dostawców oprogramowania), infrastruktura obliczeniowa i chmurowa (ocena dostawców usług chmurowych i serwerów oraz zasad dostępu do danych) czy sprzęt teleinformatyczny (ocena dostawców komputerów i urządzeń mobilnych). Raportowanie powinno obejmować także ocenę zdolności jednostki do zmiany dostawców poszczególnych urządzeń i usług. Przykład istniejących ram o zbliżonym charakterze może stanowić austriacki Kompas Suwerenności Cyfrowej (Bundesministerium Finanzen, Bundesministerium Inneres, Digital Austria, 2023).

Wdrożenie oceny zależności cyfrowych nie miałoby na celu pełnego uniezależnienia od pozazuropejskich dostawców technologii cyfrowych. Chodziłoby raczej o zrozumienie gdzie występują istotne zależności, na podstawie których można budować świadomość zagrożeń oraz podejmować kolejne decyzje, takie jak budowanie interoperacyjności systemów, tworzenie rozwiązań zapasowych, poszukiwanie bezpiecznych i suwerennych alternatyw czy w końcu projektowanie polityk publicznych na podstawie danych. Taka ustandaryzowana ocena przyniosłaby więc korzyść zarówno na szczeblu lokalnym, krajowym, jak i całej wspólnoty europejskiej.

REKOMENDACJA 4.

Wprowadzenie pomiaru suwerenności cyfrowej na poziomie lokalnym – w jednostkach samorządu terytorialnego, jednostkach edukacyjnych czy opieki zdrowotnej. W tym celu należy wypracować jednolite ramy i kryteria pomiaru. Przykładowo pomiar może dotyczyć kwestii cyberbezpieczeństwa w samorządach, narzędzi biurowych stosowanych w programach edukacyjnych czy sposobu przechowywania danych w sektorze medycznym.

Operacjonalizacja

Pomiar mógłby się odbywać w cyklu rocznym, jednak z rotacją instytucji (podobnie jak to ma miejsce w przypadku badania e-Government Benchmark, gdzie co roku badana jest inna grupa usług publicznych), co ograniczałoby obciążenia administracyjne. Dane powinny być zbierane w sposób zapewniający porównywalność między krajami. Przykładem zastosowanej miary może być obecność modułów poświęconych otwartym pakietom aplikacji w programach nauczania (Klekowski, 2025).

Znaczenie dla Polski

Regularny pomiar zależności cyfrowych w samorządach, edukacji i ochronie zdrowia uzupełnia cele Strategii cyfryzacji Polski do 2035 r. w zakresie zapewniania suwerenności technologicznej.

Powiązanie z innymi politykami UE

Rekomendacja wpisuje się we wszystkie działania związane z odbudową europejskiej suwerenności cyfrowej oraz uzupełnia działania i miary stosowane na poziomie całej wspólnoty i państw członkowskich. Łączy się też z programami rozwoju kompetencji cyfrowych (uwzględnienie w nich narzędzi *open source* lub alternatyw wobec obecnie dominujących rozwiązań) czy cyfryzacją w ochronie zdrowia.

Umiejętności cyfrowe

W kwestii umiejętności cyfrowych za Klekowskim (2025) zwracamy uwagę przede wszystkim na specjalistów ICT – osoby w dużej mierze odpowiadające za wybory dokonywane w warstwie wykorzystywanych technologii w europejskich firmach i instytucjach.

Dotychczas przyjęte miary odnoszące się do specjalistów ICT nie uwzględniają aspektu zależności technologicznych. Obecnie liderzy rynku cyfrowego dominują także obszar szkoleń ICT i oferują szkolącym się specjalistom możliwość uzyskania powszechnie uznawanych certyfikatów poświadczających kompetencje (Klekowski, 2025). Dostawcy oprogramowania, poprzez zapewnianie dostępnych i szeroko akceptowanych szkoleń, wchodzenie we współpracę z instytucjami publicznymi czy szkołami wyższymi, co prawda skutecznie podnoszą poziom cyfryzacji, ale także realizują cele biznesowe, m.in. zwiększając rozpoznawalność swojej oferty i budując komfort użytkowania wśród przeszkolonych użytkowników. Efektem jest zwiększona skłonność do późniejszego wybierania właśnie tych rozwiązań technologicznych przez specjalistów ICT.

Aby stworzyć przeciwwagę do tych najsilniej rozpowszechnionych rozwiązań, które w znaczącej większości oferowane są przez dostawców pozaeuropejskich, warto wspierać rozpowszechnianie certyfikacji odnoszącej się do systemów otwartoźródłowych oraz ich późniejszą akceptację przez pracodawców. Dobrym krokiem wydaje się promowanie i dofinansowywanie takiej certyfikacji w szkołach średnich o profilu technicznym, uczelniach i administracji publicznej, jak i oferowanie preferencyjnych warunków dla specjalistów ICT w ramach podnoszenia ich kompetencji.

REKOMENDACJA 5.

Uruchomienie publicznego wsparcia certyfikacji umiejętności wykorzystania otwartoźródłowych systemów IT, w tym finansowanie kursów zakończonych certyfikacją w szkołach średnich i wyższych oraz późniejszej akceptacji takich certyfikatów przez pracodawców z sektora publicznego, w celu ugruntowania ich wykorzystania.

Operacjonalizacja

Obecnie brakuje odpowiedniej miary, konieczne jest przeprowadzenie inwentaryzacji w zakresie pożądaných certyfikatów oraz liczby posiadających je specjalistów. Klekowski (2025) wskazuje na wykorzystanie podejścia opartego na OpenStack. Taką informację można odnieść do łącznej liczby specjalistów ICT publikowanej obecnie przez Eurostat. Problemem na tym etapie jest sposób zbierania danych o liczbie specjalistów ICT, które pochodzą z badania LSF (w Polsce jest to badanie BAEL). Charakterystyka tego badania nie daje możliwości włączenia pytań o rodzaj i liczbę uzyskanych certyfikatów.

Znaczenie dla Polski

Kwestia większego wykorzystania oprogramowania typu *open source* jest podnoszona w projekcie Strategii cyfryzacji państwa, między innymi w kontekście wzmacniania suwerenności

Powiązanie z innymi politykami UE

Unia Europejska i poszczególne kraje wspierają rozwiązania typu *open source* oraz wskazują na ich znaczenie dla rozwoju i wzmocnienia europejskich firm, a także obniżenia kosztów dla użytkowników usług cyfrowych. Jednak ostatnia kompleksowa strategia była rozpisana na lata 2020-2023 (Komisja Europejska, 2020), a obecne wspieranie tego typu rozwiązań jest rozproszone pomiędzy różne działania sektorowe.

Modyfikacje pozostałych wskaźników Cyfrowej dekady

Infrastruktura cyfrowa

W obszarze pomiaru poziomu rozwoju infrastruktury cyfrowej dla dwóch wskaźników wartości docelowe zostały niemal osiągnięte – pokrycie sieciami 5G (94 proc. w 2024 r.) oraz pokrycie sieciami o bardzo wysokiej przepustowości (82,5 proc. w 2024 r.). Pierwszy wskaźnik dotyczy obszarów zaludnionych, a w komunikacie „Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego” (Komisja Europejska, 2016) wskazywano na konieczność pokrycia również głównych szlaków transportowych. Obecnie jednak tego typu dane nie są zbierane (Komisja Europejska, 2024; 2025c), choć problem łączności na szlakach transportowych nie został rozwiązany. Dostęp do szybkiej sieci mobilnej przyczyni się do zwiększenia komfortu podróży, zapewni infrastrukturę w procesie ucyfrowienia europejskiej logistyki (m.in. poprzez zarządzanie flotą w czasie rzeczywistym) oraz umożliwi rozwój mobilności potężnej i autonomicznej (CAM) (www1).

W przypadku tego drugiego wskaźnika warto dodatkowo podkreślić, że osiągnięcie 100 proc. pokrycia wiąże się z bardzo dużymi kosztami i jest nieopłacalne ekonomicznie. W przypadkach gospodarstw domowych, które jeszcze nie uzyskały dostępu tego typu, ponieważ znajdują się w oddalonych lokalizacjach, alternatywą powinny być łącza radiowe lub pokrycie dobrej jakości siecią mobilną (Ledzion i in., 2025). Rozwiązaniem rekomendowanym z punktu widzenia dobrobytu społecznego jest zapewnienie dostępu gwarantującego funkcjonalną jakość – niezależnie czy będzie to technologia przewodowa, czy bezprzewodowa. Ponieważ tego typu rozwiązanie obejmuje również sieci radiowe i mobilne, należy zwrócić dodatkową uwagę na jakość zasięgu wewnątrz budynków.

REKOMENDACJA 6.

Wprowadzenie celu w postaci pokrycia wszystkich głównych szlaków transportowych w UE zasięgiem sieci 5G, umożliwiającym efektywne korzystanie z internetu w pociągach i pojazdach drogowych oraz na szlakach wodnych.

Operacjonalizacja

Wprowadzenie klasyfikacji szlaków transportowych w celu wyznaczenia tych, które będą objęte pomiarem⁴. Pomiar wstępny oraz regularne zbieranie danych – np. w ramach danych gromadzonych przez regulatorów rynków telekomunikacyjnych. Przykładowa miara – długość kluczowych szlaków objętych zasięgiem sieci w stosunku do całkowitej długości kluczowych szlaków transportowych w danym kraju.

REKOMENDACJA 7.

Zmiana celu zapewnienia 100 proc. gospodarstw domowych zasięgu sieci o bardzo dużej przepustowości (VHCN) oraz 100 proc. gospodarstw domowych zasięgu sieci FTTH. Celem powinno być zapewnienie funkcjonalnego dostępu do internetu dla wszystkich gospodarstw domowych, niezależnie od technologii. Cel ten powinien zostać zrealizowany do 2030 r. i nie powinien być odsuwany w czasie do 2035 r.

Operacjonalizacja

Określenie minimalnego poziomu funkcjonalnego dostępu do internetu (przez parametry techniczne⁵ lub listę usług, które muszą być dostępne⁶). Pomiar w ramach danych zbieranych przez regulatorów rynków telekomunikacyjnych, wsparty testami w różnych lokalizacjach.

Znaczenie rekomendacji 6 i 7 z punktu widzenia Polski

Polska odnotowała poziom pokrycia zasięgiem sieci 5G na poziomie 89,3 proc, a pokrycie sieciami VHCN na poziomie 83,8 proc. W ostatnich latach odnotowano dynamiczny rozwój pokrycia sieciami 5G oraz stopniowy rozwój infrastruktury światłowodowej, wspieranej funduszami europejskimi z polityki spójności i KPO. Osiągnięcie pełnego pokrycia gospodarstw domowych sieciami stacjonarnymi typu VHCN jest w Polsce w zasadzie niewykonalne, ze względu na strukturę przestrzenną zaludnienia. Zmiana celów w tym zakresie pozwoli urealnić również działania prowadzone w ramach polskich strategii cyfryzacji.

⁴ W Polsce w przypadku zobowiązań pokryciowych towarzyszących aukcji częstotliwości na potrzeby sieci mobilnych zastosowano podział na drogi krajowe i wojewódzkie, a także wyróżniono linie kolejowe, na których należy zapewnić pokrycie siecią, <https://bip.uke.gov.pl/konsultacje-i-wyniki-konsultacji/prezes-uke-oglasza-konsultacje-aukcji-na-7-rezerwacji-czestotliwosci-z-pasm-ponizej-1-ghz.3158.html> [dostęp: 14.11.2025].

⁵ Podejście przyjęte np. w aukcji częstotliwości w Polsce [link jak wyżej].

⁶ Podejście wykorzystane w Europejskim Kodeksie Łączności Elektronicznej.

Powiązanie z innymi politykami UE

Zapewnienie wysokiej jakości łączności wzdłuż głównych szlaków transportowych wpisuje się w założenia wzmacniania jednolitego rynku w UE, a także współgra z projektem realizacji sieci kolei dużych prędkości w Europie (Letta, 2024). Obecnie, w ramach CEF-digital, wspierany jest rozwój infrastruktury 5G wzdłuż wybranych transgranicznych szlaków komunikacyjnych w Unii Europejskiej (Trans-European Transport Network) (www3).

Cyfrowa transformacja biznesu

W obszarze cyfrowej transformacji biznesu wciąż pozostało wiele do zrobienia w zakresie obecnie wyznaczonych celów. **Rekomendujemy jednak ich modyfikację w celu przesunięcia akcentu na efekty prowadzonych działań (*exity* start-upów), większe skupienie na przyszłych technologiach (B+R) oraz pełniejsze monitorowanie całej populacji przedsiębiorstw (mikroprzedsiębiorstwa).**

Proponowane przez program Droga ku cyfrowej dekadzie założenie wspierania cyfrowej innowacyjności i suwerenności poprzez zamykanie luki innowacyjnej między Unią Europejską a Stanami Zjednoczonymi i Chinami jest obecnie mierzone poprzez cel podwojenia liczby europejskich „jednorożców”, czyli start-upów i *scale-upów*, które przekroczyły swoją wyceną wartość 1 mld USD. Liczba przedsiębiorstw, które odniosły tego rodzaju sukces ma stanowić o zdolnościach UE do tworzenia środowiska innowacyjnego poprzez promowanie transferu technologii, angażowanie środków publicznych oraz przyciąganie inwestycji kapitału prywatnego. Wskaźnikowi temu umyka natomiast podnoszona w raporcie o stanie unijnej transformacji cyfrowej (Komisja Europejska, 2025a) zdolność do skutecznego przeciwdziałania przenoszeniu się podmiotów innowacyjnych poza Unię Europejską. Utrzymanie obecności tych przedsiębiorstw, poprzez stworzenie odpowiednich warunków do prowadzenia działalności, jest kluczowe pod względem budowania europejskiej suwerenności.

Miara alternatywna wobec liczby jednorożców może odnosić się do odsetka europejskich start-upów technologicznych, które dokonały *exitu* w Europie, a nie na rynkach poza UE, np. w USA. Taka miara, choć również niedoskonała, pozwala na relatywną ocenę atrakcyjności rynku europejskiego dla podmiotów innowacyjnych, a nie jedynie nominalny pomiar liczby przedsiębiorstw.

REKOMENDACJA 8.

Zastąpienie wskaźnika liczby europejskich jednorożców odsetkiem start-upów, które dokonały *exitu* na rynkach europejskich. Przez *exit* rozumiemy przy tym wejście na giełdę (IPO) lub sprzedaż przedsiębiorstwa podmiotowi z kapitałem europejskim.

Operacjonalizacja

Określenie poziomu bazowego oraz docelowego może zostać dokonane na podstawie danych z istniejących i wykorzystywanych przez KE baz danych, takich jak *dealroom* czy *crunchbase*. Miarą ambicji może być np. podwojenie wskaźnika obliczonego dla 2024 r.

Znaczenie dla Polski

Polskie start-upy doświadczają podobnego problemu jak te z innych państw UE – ucieczki na rynki zagraniczne i pozaeuropejskie w celu rozwijania biznesu po początkowej fazie wzrostu. Wzmocnienie polskiego i europejskiego rynku będzie sprzyjało również firmom tworzącym w Polsce oraz utrzymywaniu kapitału i wiedzy w Polsce i UE. Podobne cele realizuje również ogłoszony jesienią 2025 r. program Innovate.Poland ([www9](http://www9.innovate.poland.eu)).

Powiązanie z innymi politykami UE

Realizacja tego celu wymaga pogłębienia rynku kapitałowego w Europie – rozwoju giełd, większej dostępności kapitału w dużych korporacjach. Jest zatem powiązane przede wszystkim z budową unii oszczędności i inwestycji. W zaprezentowanej wiosną 2025 r. strategii Komisja Europejska (2025d) diagnozuje problem ze wzrostem innowacyjnych firm w Europie oraz brakiem wystarczających możliwości wyjścia z inwestycji, a także wskazuje działania, zamierza podjąć by te problemy przetrącić.

Fakt pozostawania Europy w tyle wyścigu technologicznego przejawia się nie tylko stopniem wykorzystania technologii cyfrowych, ale również (a może nawet przede wszystkim) zaangażowania środków prywatnych w tworzenie nowych rozwiązań w najszybciej rozwijających się sektorach. Badania prowadzone regularnie przez JRC (Nindl i in., 2024) wskazują, że europejskie firmy odstają przede wszystkim w zakresie struktury sektorowej wydatków na B+R (Święcicki, 2025). W 2023 r. firmy z UE odpowiadały jedynie za 8 proc. globalnych wydatków na B+R w sektorach oprogramowania i usług komputerowych (*Computer software and services*) oraz sprzętu technologicznego i wyposażenia (*Technology hardware & equipment*), chińskie za 15,2 proc., a amerykańskie aż za 66,4 proc. Z kolei największe europejskie firmy wydają się z sektora motoryzacyjnego. Biorąc pod uwagę znaczenie przemówych technologii cyfrowych warto stymulować zwiększenie europejskich prywatnych wydatków na ten cel.

REKOMENDACJA 9.

Wprowadzenie wskaźnika do pomiaru odsetka wydatków na B+R w sferze oprogramowania komputerowego, usług i sprzętu ponoszonych przez europejskie firmy oraz celu w tym zakresie, np. na poziomie dwukrotnie wyższym niż obecnie (16 proc. zamiast 8 proc. obecnie).

Operacjonalizacja

Odpowiednie dane są zbierane i publikowane corocznie przez JRC (www2), a następnie prezentowane w podziale na państwa, regiony świata oraz sektory. Nasza propozycja obejmuje dane o wydatkach na badania i rozwój dla krajów UE (region: UE) dla kategorii *Computer software and services* oraz *Technology hardware & equipment* w porównaniu z wydatkami wszystkich klasyfikowanych firm w tych dwóch sektorach. Opcjonalnie można wziąć pod uwagę rozszerzenie tej kategorii o telekomunikację (*Fixed line telecommunications, Mobile telecommunications*).

Znaczenie dla Polski

Wśród 2000 firm największych pod względem wydatków na B+R nie ma obecnie jednostek polskich, trzy firmy znajdują się w oddzielnej klasyfikacji 800 firm z UE. W związku z tym wdrożenie tej zmiany nie ma istotnego znaczenia z punktu widzenia rozwoju Polski.

Powiązanie z innymi politykami UE

Wszelkie strategie, których celem jest pobudzenie europejskiego rynku cyfrowego (od Apply AI strategy, przez EU Chips Act, po projekty IPCEI, takie jak IPCEI ME/CT) (www8) będą wpływały na realizację tego celu.

Analizując pozostałe wskaźniki do pomiaru cyfrowej transformacji biznesu (odsetek firm korzystających z AI, chmury obliczeniowej, analityki danych), należy zwrócić uwagę, że obecne cele nie uwzględniają komponentu suwerenności. O ile w krótkim okresie to rozpowszechnienie nowych technologii będzie odpowiadało za wzrost produktywności w Europie (Święcicki, Witczak, 2025a; www3), o tyle długoterminowe bezpieczeństwo wymaga wzmocnienia odporności cyfrowej wszystkich sektorów gospodarki. Na tym etapie proponujemy pozostawienie obecnych wskaźników i uzupełnienie katalogu celów o wykorzystanie koncepcji stosu technologicznego, co opisaliśmy w dalszej części opracowania.

Ważną modyfikacją, jaką można wprowadzić do monitorowania poziomu cyfryzacji w UE, jest uwzględnienie w badaniach mikroprzedsiębiorstw. Obecne obowiązkowe badania prowadzone na firmach mających przynajmniej 10 zatrudnionych pomijają znaczną część gospodarki, odpowiadającą za 19,2 proc. wartości dodanej oraz 30,1 proc. zatrudnienia (www7).

REKOMENDACJA 10.

Rozszerzenie obowiązkowych badań poziomu cyfryzacji firm o mikroprzedsiębiorstwa (zatrudniające 0-9 pracowników).

Operacjonalizacja

Badanie takie może być włączone w regularny program badań statystycznych lub realizowane odrębnie, np. w większych odstępach czasu. Badanie należy prowadzić zgodnie z obecnymi wytycznymi Eurostat (2023) dla nieobowiązkowego badania cyfryzacji w mikroprzedsiębiorstwach, aby zachować spójność i porównywalność danych.

Znaczenie dla Polski

Z dostępnych badań wynika, że polskie mikrofirmy często bardziej intensywnie korzystają z technologii cyfrowych niż np. małe firmy (Lesiak, Świącicki, Witczak, 2025). Jednocześnie polskie mikroprzedsiębiorstwa odstają pod względem produktywności od europejskich partnerów w większym stopniu niż firmy większe (Błoński, 2021). Wprowadzenie regularnych badań mikroprzedsiębiorstw pozwoli lepiej adresować polityki publiczne i da pełniejszy obraz poziomu cyfryzacji w poszczególnych państwach członkowskich i w UE.

Powiązanie z innymi politykami UE

Rekomendacja jest spójna z programem Cyfrowej dekady i zwiększa dokładność monitorowania transformacji cyfrowej. Uzupełnia także ramy europejskich statystyk wykorzystania ICT w biznesie, które obecnie zakładają dowolność ze strony państw członkowskich w pomiarze wykorzystania technologii ICT w przedsiębiorstwach zatrudniających do 9 pracowników.

Cyberbezpieczeństwo

Cyberbezpieczeństwo jest jednym z obszarów, których obecnie nie bierze się pod uwagę w Cyfrowej dekadzie, ale jest analizowane w ramach odrębnych działań, w tym prowadzonych przez ENISA (2024a). Obszar ten jest bez wątpienia kluczowy dla skutecznej transformacji cyfrowej, zarówno z punktu widzenia celów gospodarczych, jak i społecznych. Kwestie cyberbezpieczeństwa są ujęte w innych badaniach, w kontekście bezpieczeństwa UE warto podkreślić przede wszystkim badania prowadzone przez ENISA (2024a). Zaproponowany tam zestaw wskaźników (ENISA, 2024b) obejmuje zarówno dane dotyczące realizowanych działań w zakresie cyberbezpieczeństwa w firmach, umiejętności obywateli, wydatki na badania i rozwój czy poziom dojrzałości administracji krajowych w zakresie cyberbezpieczeństwa. Wprawdzie w publicznie dostępnych raportach nie ma pełnych informacji z badania, jednak w naszej opinii tworzenie równoległego systemu pomiaru poziomu cyberbezpieczeństwa nie jest zasadne.

Jednocześnie nieobecnym w tym badaniu obszarem jest poziom cyberbezpieczeństwa mierzony na poziomie samorządów. Na tym poziomie odbywa się większość kontaktów obywateli z administracją i to one mogą stać się słabym ogniwem w strukturach obrony przed cyberzagrożeniami.

W Polsce realizowany był program Cyberbezpieczny samorząd (współfinansowany ze środków FERC), którego celem było podniesienie poziomu bezpieczeństwa informacji administracji publicznej przez dofinansowanie działań w jednostkach samorządu terytorialnego (www4). W ramach tego programu wypracowano poradniki dla JST, a także wprowadzono obowiązek dokonania audytu przez wszystkie jednostki samorządu terytorialnego biorące udział w projekcie (czyli w praktyce niemal wszystkie JST w Polsce).

REKOMENDACJA 11.

Wprowadzenie oceny stopnia dojrzałości w domenie cyberbezpieczeństwa na poziomie samorządów.

Operacjonalizacja

Obecnie brakuje odpowiedniego wskaźnika, jednak możliwe jest wykorzystanie doświadczeń z prowadzonego w Polsce projektu Cyberbezpieczny samorząd obejmującego m.in. audyt jednostek samorządu terytorialnego biorących udział w badaniu.

Znaczenie dla Polski

Jak wspominaliśmy, wzmocnienie cyberbezpieczeństwa samorządów jest jednym z działań obecnie realizowanych w Polsce. Przeniesienie pomiaru tego stanu na poziom całej UE może ułatwić staranie się o środki europejskie, może też być szansą na promowanie najlepszych praktyk z Polski w innych krajach (m.in. projekt Cyberbezpieczny samorząd).

REKOMENDACJA 12.

Wykorzystanie wskaźników EU-Cybersecurity Index rozwijanych przez ENISA jako dodatkowego wskaźnika mierzącego poziom cyberbezpieczeństwa na poziomie UE (ENISA, 2025).

Operacjonalizacja

Wskaźnik mierzony i publicznie dostępny na poziomie UE raz na dwa lata (pierwszy pomiar w 2024 r.) (ENISA, 2025). Szczegółowe wartości indeksu dla poszczególnych państw, pozwalające na tworzenie sprecyzowanych rekomendacji, są dostępne dla odpowiednich jednostek krajowych – ten aspekt przełożenia strategii na konkretne działania musiałby zapewne pozostać niepubliczny.

Jako alternatywne podejście proponujemy uwzględnienie kwestii cyberbezpieczeństwa w bardziej okrojonym zakresie, przy wykorzystaniu danych dostępnych publicznie. Takie podejście skupiałoby się na szkoleniach i certyfikacji specjalistów (z myślą o poprawie sytuacji przedsiębiorstw). Jest to też podejście rekomendowane przez ekspertów ENISA (www5).

REKOMENDACJA 12A.

Wykorzystanie wskaźników do pomiaru poziomu umiejętności (potwierdzonych uzyskanymi certyfikatami) w zakresie cyberbezpieczeństwa, zgodnych z Europejskimi Ramami Kompetencji w zakresie Cyberbezpieczeństwa (ECSF) (www6), wśród pracowników (potwierdzonych odpowiednimi certyfikatami).

Operacjonalizacja

Obecnie brakuje odpowiedniego wskaźnika, do pomiarów można wykorzystać liczbę udzielonych certyfikatów zgodnych z profilami ECSF. Wartością docelową może być np. 600 tys. certyfikowanych osób (wartość luki na rynku specjalistów z zakresu cyberbezpieczeństwa w 2024 r. szacowanej na podstawie: Święcicki, Karolak, 2025).

Znaczenie dla Polski

Strategia cyfryzacji państwa podkreśla znaczenie rozwoju programów certyfikacji cyberbezpieczeństwa, a działania takie są już obecnie podejmowane przez NASK.

Powiązanie z innymi politykami UE

Zapewnienie wysokiego poziomu cyberbezpieczeństwa w UE jest przedmiotem wielu działań i celem polityk publicznych – w tym chociażby dyrektywy NIS2, ustanowienia europejskiego centrum kompetencji w zakresie cyberbezpieczeństwa czy Cybersecurity Act.

Bibliografia

- Błoński, Ł. (2021), *Pułapka małej skali. O produktywności polskich firm*, Polski Instytut Ekonomiczny, Warszawa.
- Bria, F., Timmers, P., Gernone, F. (2025), *EuroStack – A European alternative for digital sovereignty*, Bertelsmann Stiftung, Gütersloh.
- Bonnet, P., Ciani, A. (2023), *Applying the SCAN methodology to the Semiconductor Supply Chain*, JRC Working Papers in Economics and Finance, No. 8, Komisja Europejska, Ispra.
- Bundesministerium Finanzen, Bundesministerium Inneres, Digital Austria (2023), *Digitaler Aktionsplan: Digitale Souveränität für Österreich*, Wien.
- Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie” do 2030 r. (Dz.U. L 323 z 19.12.2022), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32022D2481> [dostęp: 24.11.2025].
- Draghi, M. (2024), *The Future of European Competitiveness – A Competitiveness Strategy for Europe*.
- ENISA (2024a), *2024 Report on the State of the Cybersecurity in the Union*, <https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union> [dostęp: 14.11.2025].
- ENISA (2024b), *EU Cybersecurity Index: Framework and methodological note*, https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf [dostęp: 14.11.2025].
- ENISA (2025), *THE EU-Cybersecurity Index 2024: EU-level insights and next steps*, https://www.enisa.europa.eu/sites/default/files/2025-06/The%20EU%20Cubersecurity%20Index%202024_en_0.pdf [dostęp: 14.11.2025].
- Eurostat (2023), *European businesses statistics compilers' manual for ICT usage and e-commerce in enterprises*, Luksemburg, <https://ec.europa.eu/eurostat/documents/3859598/18369750/KS-GQ-23-012-EN-N.pdf/20fb6a79-2c43-df3d-1551-7366c72f5f8c?version=2.0&t=1706102581439> [dostęp: 28.11.2025].
- Garcia, W.C., Ho, V. (2025), *EXternal Vulnerability Index (EXVI)*, Single Market Economics Briefs, Nr 14, European Commission, Bruksela.
- Klekowski, T. (2025), *W dążeniu do suwerenności cyfrowej: Mapa technologicznych zależności Polski i Europy*, THINKTANK.
- Komisja Europejska (2016), *Łączność dla konkurencyjnego jednolitego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, COM(2016) 587 final, Bruksela.

- Komisja Europejska (2024), *How to master Europe's digital infrastructure needs?*, White Paper, COM(2024) 81 final, Bruksela.
- Komisja Europejska (2025a), *State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, COM(2025) 290 final, Bruksela.
- Komisja Europejska (2025b), *Cloud Sovereignty Framework*, Wersja 1.2.1, Luksemburg, https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf [dostęp: 14.11.2025].
- Komisja Europejska (2025c), *5G Observatory*, Raport, <https://digital-strategy.ec.europa.eu/en/policies/5g-observatory> [dostęp: 14.11.2025].
- Komisja Europejska (2025d), *Unia oszczędności i inwestycji. Strategia na rzecz zwiększenia zamożności obywateli i konkurencyjności gospodarczej w UE*, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, COM(2025) 124 final, Bruksela.
- Ledzion, B., Miller, A., Kwinta, J., Krygowska, N., Świącicki, I. (2025), *Ewaluacja ex post realizacji celów Programu Operacyjnego Polska Cyfrowa na lata 2014-2020*, Raport Końcowy, https://www.rozwojcyfrowy.gov.pl/media/156083/POPC_Raport_koncowy_expost_14082025.pdf#page=182.08 [dostęp: 14.11.2025].
- Lesiak, M., Świącicki, I., Witczak, J. (2025), *AI w polskich przedsiębiorstwach*, Point Paper, nr 5, Polski Instytut Ekonomiczny, Warszawa.
- Letta, E. (2024), *Much More Than a Market. Speed, Security, Solidarity. Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens*, <https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf> [dostęp: 27.11.2025].
- Ministerstwo Cyfryzacji (2025a), *Polska w grze o przyszłość: Polityka dla sektora półprzewodników 2025+*, <https://www.gov.pl/attachment/cb1c8d8c-1aa8-4645-9201-0f2252510559> [dostęp: 21.11.2025].
- Ministerstwo Cyfryzacji (2025b), *Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku*, <https://www.gov.pl/web/cyfryzacja/polityka-rozwoju-sztucznej-inteligencji-w-polsce-do-2030-roku--bezpieczne-i-odpowiedzialne-wykorzystanie-sztucznej-inteligencji> [dostęp: 21.11.2025].
- Ministerstwo Cyfryzacji (2025c), *Strategia cyfryzacji państwa*, dokument do konsultacji, <https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-panstwa---startuja-ponowne-konsultacje-projektu> [dostęp: 21.11.2025].
- Nindl, E., Napolitano, L., Confraria, H., Rentocchini, F., Fako, P., Gavigan, J., Tuebke, A. (2024), *The 2024 EU Industrial R&D Investment Scoreboard*, Publications Office of the European Union, Luksemburg, <https://data.europa.eu/doi/10.2760/0775231>, JRC140129 [dostęp: 21.11.2025].

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1252 z dnia 11 kwietnia 2024 r. w sprawie ustanowienia ram na potrzeby zapewnienia bezpiecznych i zrównoważonych dostaw surowców krytycznych oraz zmiany rozporządzeń (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1724 i (UE) 2019/1020 (Dz.U. L, 2024/1252, 3.5.2024), <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32024R1252> [dostęp: 27.11.2025].
- Świącicki, I. (2025), *Europa pozostaje w tyle za USA i Chinami w dziedzinie B+R*, „Tygodnik Gospodarczy PIE”, nr 1, Polski Instytut Ekonomiczny, Warszawa, https://pie.net.pl/wp-content/uploads/2025/01/Tygodnik-PIE_1-2025.pdf [dostęp: 21.11.2025].
- Świącicki, I., Karolak, M. (2025), *Methods of Systemic Funding for Cybersecurity Investments in the EU*, Policy Paper, No. 1, Polish Economic Institute, Warsaw, https://pie.net.pl/wp-content/uploads/2025/03/PP-1-2025_Cybersecurity-Discussion-ENG-4.03.2025.pdf [dostęp: 4.12.2025].
- Świącicki, I., Witczak, J. (2023), *Jak osiągnąć cele cyfrowej dekady w Polsce?*, Policy Paper, nr 6, Polski Instytut Ekonomiczny, Warszawa, https://pie.net.pl/wp-content/uploads/2024/03/PP-6-2023_Cyfrowa-dekada-w-PL.pdf [dostęp: 24.11.2025].
- Świącicki, I., Witczak, J. (2025a), *W poszukiwaniu priorytetów rozwoju AI w Polsce*, Policy Paper, nr 5, Polski Instytut Ekonomiczny, Warszawa, https://pie.net.pl/wp-content/uploads/2025/06/PIE_Policy-Paper_W-poszukiwaniu-priorytetow-rozwoju-AI-w-Polsce.pdf [dostęp: 24.11.2025].
- Świącicki, I., Witczak, J. (2025b), *Europa próbuje odbudować suwerenność technologiczną*, Tygodnik Gospodarczy, nr 45, Polski Instytut Ekonomiczny, Warszawa, https://pie.net.pl/wp-content/uploads/2025/11/Tygodnik-PIE_45-2025.pdf [dostęp: 24.11.2025].
- (www1) <https://digital-strategy.ec.europa.eu/en/policies/connected-and-automated-mobility> [dostęp: 14.11.2025].
- (www2) https://iri.jrc.ec.europa.eu/rd_monitoring [dostęp: 21.11.2025].
- (www3) <https://digital-strategy.ec.europa.eu/en/policies/cross-border-corridors> [dostęp: 14.11.2025].
- (www4) <https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad2> [dostęp: 14.11.2025].
- (www5) <https://www.enisa.europa.eu/sites/default/files/2025-10/Cybersecurity%20Skills%20Panel%20-%20Expert%20Perspectives.pdf> [dostęp: 14.11.2025].
- (www6) <https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf> [dostęp: 14.11.2025].
- (www7) <https://www.efta.int/sites/default/files/uploads/2025-03/key%20figures%20on%20european%20business-KSET24001ENN.pdf> [dostęp: 21.11.2025].
- (www8) <https://ipcei-me-ct.eu/> [dostęp: 21.11.2025].
- (www9) <https://innovatepoland.pl/> [dostęp: 28.11.2025]

Polski Instytut Ekonomiczny

Polski Instytut Ekonomiczny to publiczny *think tank* ekonomiczny z historią sięgającą 1928 roku. Jego obszary badawcze to przede wszystkim makroekonomia, energetyka i klimat, handel zagraniczny, foresight gospodarczy, gospodarka cyfrowa i ekonomia behawioralna. Instytut przygotowuje raporty, analizy i rekomendacje dotyczące kluczowych obszarów gospodarki oraz życia społecznego w Polsce, z uwzględnieniem sytuacji międzynarodowej.