

Stanowisko Rady ds. Cyfryzacji w sprawie suwerenności technologicznej Polski i Unii Europejskiej – rekomendacje

1. Jak rozumiemy suwerenność technologiczną na poziomie państwa/polityki państwa?

W obliczu gwałtownie zmieniającej się sytuacji geopolitycznej, a zwłaszcza krytycznych zagrożeń ujawnionych przez wojnę w Ukrainie oraz destabilizację globalnych łańcuchów dostaw, zwiększa się świadomość tego, że suwerenność technologiczna jest fundamentem bezpieczeństwa i odporności państwa. Nie oznacza ona izolacji ani pełnej autonomii technologicznej. Rozumiemy ją jako budowanie odporności, niezależności i strategicznej sprawczości Polski oraz Unii Europejskiej w świecie pełnym napięć. Jej istotą jest eliminowanie jednostronnych zależności oraz dywersyfikacja dostawców. Suwerenność to strategiczna zdolność Polski i Unii Europejskiej do kontrolowania, audytowania oraz elastycznego zastępowania krytycznych technologii i infrastruktury danych wszędzie tam, gdzie decydują one o naszej odporności i konkurencyjności. Polityka państwa w tym zakresie nie polega na odcinaniu się od zewnętrznych partnerów, lecz na eliminowaniu jednostronnych zależności i dywersyfikacji dostawców. Co kluczowe, tak rozumiana suwerenność jest w pełni możliwa do pogodzenia z budowaniem odporności w oparciu o świadomą, partnerską współpracę międzynarodową. Tylko poprzez rozwijanie własnych i europejskich kompetencji oraz mądre sojusze możemy skutecznie chronić gospodarkę i społeczeństwo przed szantażem cyfrowym, zabezpieczając odporność i konkurencyjność kraju i szerzej Unii Europejskiej.

Polska buduje tę odporność w oparciu o silne fundamenty: prężny sektor ICT, dojrzałą i dobrze rozwiniętą łączność stacjonarną, innowacje w obszarze nowych technologii, również z wykorzystaniem AI, osiągnięcia w sferze cyberbezpieczeństwa oraz wysoki poziom cyfryzacji wybranych usług publicznych i znaczące środki publiczne na transformację cyfrową. Zgodnie z raportem Komisji Europejskiej „Digital Decade 2025”, polska mapa drogowa obejmuje 55 działań o budżecie 12,4 mld euro, tj. 1,47% PKB; dodatkowo 7,5 mld euro z KPO i 5,7 mld euro z funduszy spójności ma wspierać transformację cyfrową. Jednocześnie Polska pozostaje strukturalnie zależna od zagranicznych dostawców w zakresie chmury, oprogramowania biurowego, cyberbezpieczeństwa, narzędzi komunikacyjnych, półprzewodników, modeli AI i platform edukacyjnych. KE wskazuje, że cała UE zależy od państw spoza Unii w ponad 80% kluczowych produktów, usług, infrastruktury i własności intelektualnej w obszarze cyfrowym. Szczególnym wyzwaniem jest asymetria między tempem cyfryzacji państwa a zdolnością państwa do kontrolowania technologii, na których ta cyfryzacja się opiera. Polska korzysta z globalnych technologii, ale zbyt rzadko posiada realne narzędzia audytu, migracji, zastąpienia dostawcy, kontroli nad danymi oraz wpływu na rozwój produktu. Ryzyko to dotyczy zwłaszcza chmury (w szczególności obliczenia i przestrzenie składowania danych), cyberbezpieczeństwa, AI, narzędzi komunikacyjnych, półprzewodników, edukacji cyfrowej i systemów używanych przez administrację centralną i lokalną.

Największym ryzykiem dla Polski nie jest samo korzystanie z technologii globalnych dostawców, lecz brak zdolności do zarządzania zależnościami, m.in. brak mapy krytycznych zależności, słabe kryteria zakupowe i świadomość zakupowa zamawiających w sektorze publicznym, niedostateczna interoperacyjność, od wielu lat uzależnienie kompetencji (młodych) ludzi od zamkniętych ekosystemów, roczność budżetu utrudniająca przemysłowe zakupy oraz niewystarczająca koordynacja zamówień publicznych, zakupów poza PZP i zakupów spółek Skarbu Państwa.

Ryzykiem nie jest samo pochodzenie dostawcy, lecz brak kontroli nad zależnościami: brak planu wyjścia, brak interoperacyjności, brak własności i kontroli nad danymi, brak alternatywnego dostawcy oraz brak kompetencji po stronie zamawiającego. Dlatego kryteria suwerennościowe nie powinny oznaczać automatycznej preferencji dla firm polskich, lecz premiowanie rozwiązań tworzących wartość, bezpieczeństwo, odporność i kompetencje w Polsce oraz UE.

W dniu 3 czerwca 2026 r. Komisja Europejska przedstawiła pakiet suwerenności technologicznej obejmujący m.in. Chips Act 2.0, Cloud and AI Development Act oraz strategię open source, koncentrując się na półprzewodnikach, AI, chmurze i otwartym oprogramowaniu. Inne państwa europejskie podejmują działania praktyczne: Francja rozwija kwalifikację SecNumCloud dla chmury zaufanej, Niemcy poprzez ZenDiS i openCode budują kompetencje open source w administracji, Niderlandy postulują wspólne europejskie zasady suwerenności chmurowej, a Dania rozpoczęła ograniczanie zależności administracji od zamkniętych pakietów biurowych.

2. Suwerenność technologiczna jako horyzontalne kryterium polityki państwa w zakresie cyfryzacji, edukacji, cyberbezpieczeństwa, polityki przemysłowej, zamówień publicznych, nauki, innowacji, obronności i polityki europejskiej.

Suwerenność technologiczna powinna być osadzona w praktyce państwa przez następujące mechanizmy:

- a. strategiczne zarządzanie zależnościami,
- b. mądre zakupy publiczne,
- c. rozwój kompetencji,
- d. otwarte standardy i open source,
- e. wzmacnianie krajowego i europejskiego ekosystemu dostawców,
- f. rozwój krajowej i europejskiej bazy przemysłowo-technologicznej w wybranych obszarach strategicznych, w szczególności AI, cyberbezpieczeństwie, zarządzaniu danymi, ale także na przykład w dronach, robotyce, technologiach kwantowych, mikroelektronice, infrastrukturze obliczeniowej.

3. Kontekst strategiczny

Mając na uwadze wyżej wskazane wyzwania, Rada ds. Cyfryzacji rekomenduje przyjęcie Krajowej Mapy Suwerenności Technologicznej 2027–2030. Dokument ten powinien precyzyjnie zdefiniować technologie krytyczne dla funkcjonowania państwa, obejmując obszary od chmury, centrów danych i cyberbezpieczeństwa, przez tożsamość cyfrową, łączność, AI, modele językowe i półprzewodniki, aż po technologie kwantowe oraz systemy kluczowe dla zdrowia, energetyki, edukacji i samorządów. Fundamentem Mapy powinno być jasne podzielenie tych zasobów na trzy kategorie:

- technologie wymagające pełnej, autonomicznej kontroli państwa;
- technologie, dla których wystarczający jest nadzór na poziomie europejskim; oraz
- rozwiązania globalne, z których korzystanie będzie dopuszczalne pod warunkiem rygorystycznego spełnienia wymogów bezpieczeństwa, audytowalności, pełnej interoperacyjności i posiadania gotowego planu wyjścia (tzw. exit planu).

Doświadczenia ostatnich lat pokazują, że suwerenność technologiczna nie może opierać się wyłącznie na pojedynczych dużych inwestycjach zagranicznych, które mogą nie być zrealizowane (np. niezrealizowany projekt budowy Zakładu Integracji i Testowania Półprzewodników pod Wrocławiem). Polska powinna jednocześnie zabiegać o inwestycje globalne, rozwijać europejskie łańcuchy dostaw oraz budować krajowe kompetencje w niszach, w których możliwy jest szybki wzrost. W tym celu Rada ds. Cyfryzacji rekomenduje przygotowanie i przyjęcie polityki przemysłowej, uwzględniającej politykę zakupową ze środków publicznych, ukierunkowanej na rozwój polskich i europejskich zdolności technologicznych w obszarach, w których Polska powinna posiadać pełną kontrolę, może budować przewagi lub szybko nadrobić zaległości.

Przygotowanie i wdrożenie nowoczesnej polityki przemysłowej powinno stać się jednym z kluczowych elementów strategii rozwoju Polski w nadchodzących latach. Wspomniana polityka powinna być ściśle powiązana z polityką zakupową państwa, a także z wykorzystaniem środków publicznych jako narzędzi stymulowania innowacji i rozwoju krajowych kompetencji technologicznych. Podkreślenia wymaga to, że państwo nie powinno ograniczać się wyłącznie do roli regulatora i odbiorcy technologii, lecz także aktywnie kształtować popyt na rozwiązania rozwijane zarówno przez polskie i europejskie przedsiębiorstwa, przy czym w przypadku tych drugich warto zadbać, by polskie podmioty pełniły rolę kooperantów.

Szczególne znaczenie mają te obszary (sektory) gospodarki, w których Polska posiada potencjał do budowania przewag konkurencyjnych lub szybkiego nadrobienia zaległości technologicznych. Dotyczy to m.in. cyberbezpieczeństwa, sektorowych zastosowań sztucznej inteligencji, mniejszych modeli językowych dostosowanych do języka polskiego i potrzeb administracji publicznej, technologii dronowych, robotyki, technologii kosmicznych, zastosowań AI w rolnictwie, energetyce i przemyśle, a także mikroelektroniki, fotoniki oraz sensorów. Elementem kluczowym, który pozwala na wykorzystanie tego potencjału jest dobrze przygotowana infrastruktura danych i usług chmurowych, gwarantująca rozwój przy zapewnieniu bezpieczeństwa oraz zgodności z europejskimi regulacjami.

Pojedyncze duże inwestycje zagraniczne, choć pozostają ważnym elementem rozwoju gospodarczego, są uzależnione od globalnej sytuacji gospodarczej, decyzji korporacyjnych oraz czynników geopolitycznych. Uwzględniając te czynniki Polska powinna prowadzić politykę wielotorową: z jednej strony przyciągać inwestorów zagranicznych, z drugiej aktywnie uczestniczyć w budowie europejskich łańcuchów dostaw, europejskiego stosu technologicznego, a równocześnie wspierać rozwój krajowych przedsiębiorstw i kompetencji badawczo-rozwojowych.

Istotnym instrumentem realizacji tej polityki powinny być także zamówienia publiczne. Państwo i samorządy są jednymi z największych nabywców technologii w Polsce, dlatego odpowiednio projektowane postępowania zakupowe mogą tworzyć rynek dla innowacyjnych rozwiązań, rozwijanych przez krajowe podmioty. Nie chodzi przy tym o ograniczanie konkurencji, lecz o takie definiowanie potrzeb i kryteriów jakościowych, aby wspierać rozwój kompetencji strategicznych dla suwerenności, bezpieczeństwa i konkurencyjności polskiej gospodarki.

W długoterminowej perspektywie celem powinno być zwiększenie odporności gospodarki na zewnętrzne szoki technologiczne, ograniczenie uzależnienia od dostawców spoza Europy oraz budowa własnych kompetencji w kluczowych obszarach, w tym także cyfrowych. W świecie, w którym technologia staje się jednym z głównych czynników siły gospodarczej i politycznej państw, zdolność do tworzenia i rozwijania własnych rozwiązań technologicznych staje się równie istotna jak tradycyjnie rozumiane bezpieczeństwo energetyczne czy militarne.

Rada ds. Cyfryzacji ponadto rekomenduje:

- a. Wprowadzenie obligatoryjnego „testu suwerenności technologicznej” dla kluczowych systemów publicznych. Narzędzie to służyłoby do rygorystycznej oceny architektury i otoczenia prawnego wdrażanych rozwiązań jeszcze przed podjęciem decyzji zakupowych. Test weryfikowałby m.in. lokalizację i kontrolę nad danymi, jurysdykcję dostawcy, udział komponentów open source oraz odporność łańcucha dostaw, ze szczególnym uwzględnieniem ryzyka uzależnienia od jednego producenta (vendor lock-in) czy jednej jurysdykcji. Ocenie podlegałoby tacy partnerzy pod kątem możliwości przeprowadzania niezależnych audytów, pełnej interoperacyjności i przenoszalności danych, a także realności planów wyjścia (exit plan). Kluczowym elementem testu byłoby badanie możliwości zastosowania modeli dual vendor lub multi vendor, poziom niezależności od jednej jurysdykcji, możliwość niezależnego audytu mniejszych dostawców, oraz bezwzględne zapewnienie, że to sektor publiczny pozostaje wyłącznym właścicielem i dysponentem danych, przy jednoczesnym premiowaniu rozwiązań, które pozytywnie wpływają na rozwój polskiego i europejskiego ekosystemu ICT.
- b. W celu skutecznego przeciwdziałania zjawisku „sovereignty washing”, status europejskiego dostawcy suwerennych technologii powinien być uzależniony nie tylko od lokalizacji infrastruktury lub rejestracji podmiotu w UE, lecz przede wszystkim od rzeczywistej europejskiej kontroli nad własnością intelektualną, rozwojem produktu oraz strategicznymi procesami decyzyjnymi. Dostawca powinien wykazać zdolność do samodzielnego utrzymania, rozwijania i zabezpieczania kluczowych komponentów

rozwiązania na terytorium Unii Europejskiej, w szczególności poprzez wytworzenie i posiadanie praw własności intelektualnej lub innych trwałych i skutecznych tytułów prawnych zapewniających pełną kontrolę nad rozwojem technologii, dostęp do kodu źródłowego oraz możliwość jego modyfikacji i dalszego rozwoju.

Jednocześnie zasadne jest wprowadzenie obowiązkowego testu rzeczywistej kontroli (effective control test), obejmującego pełną transparentność struktury właścicielskiej aż do poziomu beneficjenta rzeczywistego (ultimate beneficial ownership – UBO) oraz ocenę bezpośrednich i pośrednich mechanizmów kontroli, w tym faktycznej kontroli korporacyjnej, strategicznej i technologicznej nad dostawcą. Rzeczywista kontrola powinna pozostawać po stronie podmiotów z Unii Europejskiej. Żaden podmiot spoza UE, samodzielnie, poprzez podmioty powiązane ani działając w porozumieniu z innymi podmiotami, nie powinien posiadać praw, uprawnień umownych lub innych instrumentów umożliwiających wywieranie decydującego, blokującego lub faktycznego wpływu na strategię przedsiębiorstwa, rozwój produktu, własność intelektualną, architekturę technologiczną, bezpieczeństwo, dane lub ciągłość działania. Ocena powinna obejmować w szczególności prawa głosu, prawa weta, skład organów spółki, umowy licencyjne, joint venture, umowy o wyłączności, finansowanie oraz inne mechanizmy zależności gospodarczej lub technologicznej. Wymogi te powinny być spełniane w sposób ciągły, z obowiązkiem notyfikowania zmian mających wpływ na ocenę kontroli. Takie rozwiązanie pozwoliłoby ograniczyć możliwość tworzenia konstrukcji formalnie spełniających kryteria europejskiego dostawcy, które pomimo lokalnej infrastruktury lub rejestracji pozostają technologicznie, kapitałowo lub decyzyjnie zależne od podmiotów spoza Unii Europejskiej.

- c. Utworzenie centralnej funkcji zarządzania zależnościami technologicznymi państwa, przy czym nie chodzi o centralne kupowanie wszystkiego, lecz o centralne zarządzanie kategoriami strategicznymi, czyli państwo powinno wiedzieć na co stawia, gdzie buduje alternatywy, gdzie akceptuje zależność, a gdzie wymaga pełnej kontroli.
- d. Wpisanie suwerenności technologicznej do polityki zakupowej państwa. Zakupy publiczne powinny być narzędziem polityki przemysłowej i bezpieczeństwa, nie wyłącznie procedurą wyboru najtańszej oferty. Kryteria suwerennościowe w zamówieniach publicznych powinny premiować nie narodowość dostawcy jako taką, lecz bezpieczeństwo, audytowalność, transparentny łańcuch dostaw, interoperacyjność, możliwość migracji, lokalne kompetencje serwisowe, udział polskich lub europejskich zespołów oraz tworzenie wartości gospodarczej w Polsce i UE.
- e. Wspieranie środkami publicznymi (krajowymi, unijnymi) lokalnej (zarówno krajowej, jak i unijnej) branży technologicznej w celu równoległego budowania własnej przewagi konkurencyjnej i zaufanych alternatyw, przy zachowaniu możliwości współpracy międzynarodowej. Europejskie firmy, nawet jeśli rozwijają wewnętrznie własne narzędzia cyfrowe, to najczęściej opierają je na rozwiązaniach chmurowych i technologiach dostarczanych przez globalne korporacje. W pierwszej połowie 2025 r. zaledwie trzy amerykańskie firmy odpowiadały za ok. 70 proc. całego rynku usług chmurowych w Europie. Na ten moment jest to najbardziej efektywne kosztowo wyjście, ale

równocześnie tworzy silne asymetrie i uzależnienia, które ograniczają suwerenność technologiczną polskich i europejskich podmiotów.

- f. Stworzenie modelu strategicznego partnerstwa państwa z firmami technologicznymi. Państwo nie powinno wyłącznie budować technologii samodzielnie ani wyłącznie kupować gotowych produktów od globalnych dostawców. Powinno umieć zamawiać rozwój technologii wspólnie z rynkiem, w tym przez dialog techniczny, zamówienia przedkomercyjne, piaskownice regulacyjne, konkursy technologiczne, partnerstwa publiczno-prywatne i wieloletnie kontrakty rozwojowe.
- g. Wzmocnienie krajowego ekosystemu open source poprzez ustanowienie zasady „open source first” w administracji tam, gdzie jest to funkcjonalnie i uzasadnione pod kątem bezpieczeństwa, a także zasadę „public money, public code” dla kodu finansowanego ze środków publicznych, z wyjątkami dla bezpieczeństwa państwa. Podobne postulaty są już przedmiotem europejskiej debaty o reformie zamówień publicznych.
- h. Wprowadzenie „paszportu produktu cyfrowego” dla systemów krytycznych. Paszport powinien dokumentować łańcuch dostaw czyli kraj pochodzenia, właściciela, zależności licencyjne, komponenty open source, miejsca przetwarzania danych, podwykonawców, zgodność z normami cyberbezpieczeństwa i plan wyjścia.
- i. Opracowanie referencyjnej architektury cyfrowej dla administracji rządowej i samorządowej, aby lokalne wdrożenia nie pogłębiały fragmentacji i zależności od pojedynczych dostawców.
- j. Podjęcie kompleksowych, skoordynowanych na poziomie państwa działań na rzecz budowy „Polskiego Stosu Technologicznego” dla administracji, obejmującego referencyjne, interoperacyjne i audytowalne komponenty. Stos ten nie powinien oznaczać jednego obowiązkowego systemu dla wszystkich, lecz zestaw referencyjnych, interoperacyjnych komponentów, standardów i dobrych praktyk, które administracja może wykorzystywać bez pogłębiania zależności od jednego dostawcy. Równocześnie warto podkreślić istotę wewnątrzunijnej integracji. Działania powinny być skupione nie tylko na budowie zamkniętego „Polskiego Stosu Technologicznego”, gdyż znacznie większy potencjał ma współpraca między państwami członkowskimi i europejskimi firmami oraz wzajemna wymiana doświadczeń i rozwijanych technologii. Kluczowe jest także aktywne włączenie się w tworzenie EuroStack, w ramach którego polskie firmy mogłyby tworzyć warstwy cyfrowego ekosystemu. Publiczne wsparcie powinno obejmować nie tylko podmioty komercyjne, ale również inicjatywy non-profit, takie jak chociażby BielikAI.
- k. Program transformacji cyfrowej MŚP oparty o polski i europejski sektor ICT: należy połączyć granty, bony cyfrowe, doradztwo, cyberbezpieczeństwo i wdrożenia AI z preferencją dla interoperacyjnych, przenoszalnych i europejskich rozwiązań, tak aby środki publiczne nie tylko finansowały zakup zagranicznych licencji, ale realnie budowały popyt na polskie i europejskie produkty, wdrożenia, integracje i kompetencje. Działania te zapobiegają wpadnięciu rodzimych firm w pułapkę uzależnienia od jednego dostawcy (vendor lock-in).

- l. Należy ograniczać sytuacje, w których bezpłatne programy edukacyjne globalnych korporacji prowadzą do trwałego uzależnienia kompetencji uczniów, studentów i przyszłych pracowników od jednego zamkniętego ekosystemu. Państwo powinno zapewnić szkołom i uczelniom neutralne technologicznie materiały dydaktyczne, środowiska open source, europejskie alternatywy oraz szkolenia dla nauczycieli.
- m. Wzmocnienie roli uczelni i publicznych jednostek badawczych jako twórców technologii, a nie wyłącznie wykonawców analiz i raportów.

Jednostki badawcze powinny mieć mierzalne cele technologiczne, benchmarki międzynarodowe, obowiązek udziału w projektach wdrożeniowych oraz ścieżkę komercjalizacji rezultatów badań. Rozwój nowoczesnej gospodarki opiera się na zdolności do tworzenia i wdrażania innowacyjnych technologii. Państwa, które osiągnęły trwałą przewagę konkurencyjną, takie jak Stany Zjednoczone, Korea Południowa, Izrael, Finlandia czy Niemcy, zbudowały silny ekosystem współpracy pomiędzy nauką, przemysłem i administracją publiczną. Kluczową rolę odgrywają w nim uczelnie wyższe oraz jednostki badawcze, które nie ograniczają się do prowadzenia badań podstawowych i opracowywania analiz, lecz aktywnie uczestniczą w tworzeniu nowych produktów, technologii i przedsiębiorstw opartych na wiedzy.

W Polsce potencjał naukowy jest znaczący, mamy wielu naukowców praktyków, jednak jego wykorzystanie pozostaje niewystarczające. Znaczna część działalności uczelni publicznych i niepublicznych i jednostek badawczych koncentruje się na przygotowywaniu ekspertyz, raportów oraz publikacji naukowych, które mają ograniczony wpływ na rozwój gospodarki. Liczba skutecznie komercjalizowanych patentów, wdrożonych technologii oraz przedsiębiorstw typu spin-off nadal pozostaje niższa niż w krajach będących liderami innowacyjności. Dlatego konieczne jest przekształcenie modelu funkcjonowania polskich instytucji naukowych w kierunku aktywnego tworzenia technologii oraz ich skutecznego wdrażania. Pierwszym elementem tej zmiany powinno być określenie mierzalnych celów technologicznych dla uczelni publicznych i niepublicznych oraz jednostek badawczych. Obecnie ocena działalności naukowej opiera się przede wszystkim na liczbie publikacji, cytowań oraz osiągnięć akademickich, które są ważnym elementem rozwoju nauki, ale nie odzwierciedlają rzeczywistego wpływu badań na gospodarkę i społeczeństwo. W nowym modelu oceny powinny znaleźć się również wskaźniki dotyczące liczby zgłoszeń patentowych, udzielonych patentów, licencji technologicznych, wdrożeń przemysłowych, utworzonych spółek technologicznych oraz wartości przychodów uzyskanych z komercjalizacji wyników badań i działalności gospodarczej. Takie rozwiązanie motywowałoby jednostki naukowe do podejmowania badań aplikacyjnych oraz ścisłej współpracy z przedsiębiorstwami. Jednocześnie nie oznaczałoby rezygnacji z badań podstawowych, które pozostają fundamentem rozwoju nauki. Kluczowe jest jednak zachowanie odpowiednich proporcji pomiędzy działalnością poznawczą a tworzeniem praktycznych rozwiązań odpowiadających na potrzeby gospodarki.

- n. Wprowadzenie benchmarków międzynarodowych jako drugiego filaru wzmocnienia roli uczelni i jednostek badawczych w tworzeniu technologii.

Każdy jednostka badawcza oraz uczelnia prowadząca działalność B+R powinny regularnie porównywać swoje osiągnięcia z najlepszymi jednostkami naukowymi w Europie i na świecie. Benchmarki powinny obejmować m.in. liczbę patentów przypadających na pracownika naukowego, wartość projektów realizowanych wspólnie z przemysłem, udział finansowania pochodzącego z działalności gospodarczej, liczbę technologii wdrożonych na rynek oraz pozycję w międzynarodowych rankingach innowacyjności. Porównywanie wyników z liderami światowymi pozwoli identyfikować obszary wymagające poprawy oraz skuteczniej planować kierunki rozwoju. Dzięki temu instytucje naukowe będą mogły korzystać z najlepszych praktyk organizacyjnych, modeli współpracy z biznesem oraz sprawdzonych metod komercjalizacji technologii.

- o. Obowiązek udziału jednostek badawczych i uczelni w projektach wdrożeniowych.

Zbyt często projekty badawcze kończą się publikacją raportu lub opracowaniem dokumentacji technicznej, bez przejścia do etapu praktycznego wykorzystania wyników badań. Tymczasem prawdziwa wartość badań ujawnia się dopiero w momencie ich zastosowania w gospodarce, administracji publicznej lub życiu społecznym. Każdy większy projekt, który nie dotyczy badań podstawowych, finansowany ze środków publicznych, powinien zawierać plan wdrożenia rezultatów oraz określenie partnera odpowiedzialnego za ich praktyczne wykorzystanie. W przypadku projektów o wysokim potencjale gospodarczym jednostki powinny aktywnie uczestniczyć w procesie budowy prototypów, testów przemysłowych, certyfikacji oraz przygotowania technologii do produkcji seryjnej. Takie podejście zwiększy efektywność wydatkowania środków publicznych i przyczyni się do szybszego rozwoju innowacyjnych przedsiębiorstw. Ważnym narzędziem wspierającym ten proces powinny stać się centra transferu technologii lub dedykowane temu spółki, funkcjonujące przy uczelniach i jednostkach badawczych. Ich rola nie może ograniczać się wyłącznie do obsługi formalnej zgłoszeń patentowych. Powinny one pełnić funkcję profesjonalnych jednostek biznesowych odpowiedzialnych za analizę potencjału rynkowego wynalazków, wyszukiwanie partnerów przemysłowych, negocjowanie umów licencyjnych oraz wspieranie tworzenia spółek spin-off i spin-out. W wielu krajach rozwiniętych centra transferu technologii zatrudniają specjalistów posiadających doświadczenie biznesowe, inwestycyjne i prawne. Dzięki temu naukowcy mogą koncentrować się na działalności badawczej, natomiast proces komercjalizacji prowadzony jest przez profesjonalnych menedżerów technologii. Podobny model powinien zostać szeroko wdrożony również w Polsce.

- p. Rozwój przedsiębiorczości akademickiej. Naukowcy powinni być zachęceni do zakładania własnych przedsiębiorstw wykorzystujących wyniki prowadzonych badań. Wymaga to uproszczenia procedur związanych z tworzeniem spółek spin-off, uregulowania kwestii własności intelektualnej oraz zapewnienia dostępu do kapitału zaangażowanego. Uczelnie powinny tworzyć inkubatory przedsiębiorczości, laboratoria demonstracyjne oraz programy mentoringowe prowadzone wspólnie z przedsiębiorcami i inwestorami. Dzięki temu możliwe będzie skrócenie drogi od pomysłu naukowego do gotowego produktu obecnego na rynku.

- q. Zmiana systemu finansowania jednostek badawczych. Obecny model w dużej mierze premiuje liczbę realizowanych projektów oraz aktywność publikacyjną. W przyszłości część finansowania powinna zależeć od rzeczywistego wpływu prowadzonych badań na rozwój gospodarczy kraju. Ocenie mogłyby podlegać między innymi przychody z licencji, liczba wdrożeń przemysłowych, wartość kontraktów realizowanych wspólnie z przedsiębiorstwami oraz udział w projektach strategicznych dla państwa. Takie rozwiązanie zwiększyłoby motywację do prowadzenia badań odpowiadających na realne potrzeby rynku. Jednocześnie nie powinno prowadzić do marginalizacji badań podstawowych, które wymagają stabilnego finansowania i stanowią źródło przyszłych przełomowych odkryć. Współpraca z przemysłem powinna mieć charakter długofalowy, a nie jedynie projektowy. Jednostki badawcze mogą pełnić rolę partnerów technologicznych przedsiębiorstw, wspólnie opracowując nowe rozwiązania od etapu koncepcji aż do wdrożenia. Szczególnie istotne jest rozwijanie współpracy w strategicznych sektorach gospodarki, takich jak energetyka, medycyna, biotechnologia, technologie kosmiczne, cyberbezpieczeństwo, sztuczna inteligencja (w tym zarządzanie danymi), elektronika, robotyka oraz technologie materiałowe.
- r. Wsparcie rozwoju międzynarodowych konsorcjów badawczych oraz zwiększanie udziału polskich jednostek naukowych w europejskich programach badawczo-rozwojowych. Udział w projektach międzynarodowych pozwala zdobywać doświadczenie, korzystać z nowoczesnej infrastruktury badawczej oraz budować trwałe relacje z najlepszymi ośrodkami naukowymi na świecie. Dzięki temu polskie technologie mogą szybciej trafiać na rynki zagraniczne.
- s. Zmiana kultury organizacyjnej państwowych jednostek badawczych. Sukces naukowy powinien być definiowany nie tylko przez publikacje i cytowania, ale także przez liczbę rozwiązań wdrożonych do praktyki gospodarczej. Pracownicy naukowcy angażujący się w komercjalizację powinni otrzymywać odpowiednie wsparcie organizacyjne oraz system motywacyjny uwzględniający udział w zyskach z wdrażanych technologii. Proces komercjalizacji powinien stać się integralnym elementem działalności każdej jednostki badawczej. Każdy projekt posiadający potencjał rynkowy powinien przechodzić przez jasno określoną ścieżkę obejmującą ocenę potencjału technologii, ochronę własności intelektualnej, przygotowanie modelu biznesowego, pozyskanie partnerów przemysłowych, testy wdrożeniowe oraz wejście produktu na rynek. Taka standaryzacja znacząco zwiększy skuteczność wykorzystania wyników badań.
- t. Przyjęcie polityki wartości danych publicznych. Polska powinna rozwijać mechanizmy pozwalające tworzyć wartość gospodarczą w kraju na bazie danych publicznych: bezpieczne przestrzenie danych, standardy API, licencje dla zastosowań komercyjnych, wsparcie dla polskich firm budujących usługi na danych publicznych oraz mechanizmy mierzenia wykorzystania danych. Celem nie jest ograniczenie otwartości danych, lecz zapewnienie, że wartość z ich wykorzystania wspiera również polską gospodarkę i administrację. Współczesna gospodarka coraz silniej opiera się na danych, które stały się jednym z najważniejszych zasobów państwa. Dane publiczne – gromadzone przez administrację rządową, samorządy, instytucje naukowe, jednostki dziedzictwa

kulturowego czy podmioty realizujące zadania publiczne – stanowią fundament rozwoju innowacyjnych usług cyfrowych, sztucznej inteligencji, analiz ekonomicznych oraz nowoczesnych modeli biznesowych. W Polsce w ostatnich latach znacząco zwiększyła się dostępność otwartych danych, jednak samo udostępnianie danych nie gwarantuje, że korzyści gospodarcze z ich wykorzystania pozostaną w kraju. Coraz częściej największymi beneficjentami publicznych zbiorów danych stają się globalne przedsiębiorstwa technologiczne dysponujące odpowiednim kapitałem, infrastrukturą obliczeniową i zaawansowanymi algorytmami, które wykorzystują udostępniane zasoby do budowania nowych technologii. Polska administracja ponosi koszty tworzenia i utrzymywania wysokiej jakości baz danych, natomiast znacząca część wartości ekonomicznej powstającej na ich podstawie może być generowana poza granicami kraju. Dlatego potrzebna jest nowoczesna polityka wartości danych publicznych, której celem będzie nie ograniczanie otwartości danych, lecz stworzenie warunków, aby ich wykorzystanie wzmacniało rozwój polskiej gospodarki, administracji oraz krajowego sektora technologicznego.

Polityka ta powinna opierać się na pięciu filarach:

- budowie bezpiecznych przestrzeni danych,
- tworzeniu jednolitych standardów API,
- opracowaniu przejrzystych zasad licencjonowania zastosowań komercyjnych,
- wspieraniu polskich przedsiębiorstw rozwijających usługi oparte na danych publicznych oraz
- wdrożeniu systemu mierzenia społecznej i gospodarczej wartości wykorzystania danych.

Dane publiczne stanowią strategiczny zasób państwa, zaś przez wiele lat dane publiczne postrzegano głównie jako element przejrzystości działania administracji. Obecnie ich znaczenie znacznie wykracza poza funkcję informacyjną. Dane dotyczące transportu, zdrowia, środowiska, geodezji, edukacji, dziedzictwa kulturowego, finansów publicznych czy statystyki państwowej są paliwem dla rozwoju gospodarki cyfrowej. Wykorzystanie tych informacji umożliwia tworzenie aplikacji transportowych, systemów prognozowania zagrożeń klimatycznych, narzędzi wspomagających diagnostykę medyczną, rozwiązań dla inteligentnych miast czy modeli sztucznej inteligencji. W praktyce dane publiczne stają się infrastrukturą równie ważną jak drogi, sieci energetyczne czy telekomunikacyjne. Państwo powinno więc prowadzić świadomą politykę zarządzania tym zasobem. Oznacza to nie tylko zapewnienie jego dostępności, lecz również rozwijanie ekosystemu, który umożliwi powstawanie innowacyjnych produktów i usług w Polsce. Szczególnie istotne jest wspieranie krajowych przedsiębiorstw, które często dysponują wysokimi kompetencjami technologicznymi, ale nie posiadają porównywalnych zasobów finansowych jak globalni konkurenci. Jednym z najważniejszych elementów polityki wartości danych publicznych powinno być tworzenie bezpiecznych przestrzeni danych (data spaces). Istotnym będzie w tym kontekście wykorzystanie aktualnego zaangażowania polskich jednostek naukowych w budowanie tego rodzaju przestrzeni

danych na poziomie europejskim (ang. Common European data spaces) i rozszerzenie ich o zastosowania krajowe i regionalne. Przestrzenie danych to środowiska umożliwiające wymianę i analizę danych pomiędzy administracją, przedsiębiorstwami, uczelniami oraz jednostkami badawczymi przy zachowaniu wysokich standardów bezpieczeństwa, ochrony prywatności oraz zgodności z przepisami prawa. W tym kontekście nie wszystkie dane mogą być udostępniane w pełni otwarcie lub do dowolnego zastosowania. W wielu przypadkach zawierają informacje wrażliwe, dane osobowe lub informacje mające znaczenie dla bezpieczeństwa państwa. Dzięki bezpiecznym przestrzeniom danych możliwe jest prowadzenie analiz bez konieczności kopiowania całych zbiorów danych czy ich niekontrolowanego rozpowszechniania. Ponadto, takie rozwiązania pozwalają rozwijać zaawansowane modele sztucznej inteligencji, badania naukowe oraz innowacyjne usługi publiczne przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa. W przyszłości mogą one obejmować między innymi sektor zdrowia, energetyki, transportu, rolnictwa, dziedzictwa kulturowego czy przemysłu. Drugim filarem polityki wartości danych publicznych powinno być stworzenie jednolitych standardów udostępniania danych za pomocą interfejsów programistycznych API, a w szczególności zapewnienie adekwatnego poziomu jakości tych danych w perspektywie zaawansowanych zastosowań. Obecnie wiele instytucji publicznych publikuje dane w różnych formatach, wykorzystuje odmienne sposoby autoryzacji oraz niejednolite modele dokumentacji technicznej. Utrudnia to przedsiębiorcom oraz programistom budowę usług opartych na danych administracji. Wprowadzenie wspólnych standardów oznaczałoby: jednolite sposoby uwierzytelniania użytkowników, wspólne formaty wymiany danych, ujednoliconą dokumentację techniczną, stabilne wersjonowanie interfejsów, wysoką dostępność usług. Standaryzacja znacząco obniży koszty tworzenia nowych produktów cyfrowych. Programiści nie będą musieli każdorazowo poznawać odmiennych rozwiązań stosowanych przez poszczególne urzędy. Ułatwi to także integrację danych z wielu źródeł oraz rozwój usług wykorzystujących jednocześnie informacje pochodzące z administracji centralnej i samorządowej. Dla administracji oznacza to również łatwiejsze utrzymanie infrastruktury oraz możliwość automatycznego monitorowania wykorzystania udostępnianych zasobów.

- u. Stworzenie systemu wspierania polskich przedsiębiorstw wykorzystujących dane publiczne. Obecnie wiele startupów oraz małych firm technologicznych posiada wysokie kompetencje w zakresie analizy danych i sztucznej inteligencji, jednak napotyka bariery związane z dostępem do infrastruktury obliczeniowej, finansowania czy specjalistycznego doradztwa. Państwo mogłoby rozwijać programy obejmujące: granty na budowę produktów wykorzystujących dane publiczne, fundusze wspierające komercjalizację innowacyjnych rozwiązań, akceleratory dla startupów, preferencyjny dostęp do infrastruktury chmurowej, programy pilotażowe realizowane wspólnie z administracją.

Jednym z największych wyzwań jest brak systematycznego monitorowania efektów wykorzystania danych publicznych. W wielu przypadkach administracja nie posiada informacji, które zbiory danych są najczęściej wykorzystywane, jakie branże z nich korzystają ani jaka wartość gospodarcza powstaje dzięki ich udostępnianiu. Dlatego polityka wartości danych powinna obejmować stworzenie systemu wskaźników

monitorujących między innymi: liczbę wykorzystań poszczególnych zbiorów danych, liczbę przedsiębiorstw korzystających z danych, liczbę produktów i usług opartych na danych publicznych, wpływ na wzrost gospodarczy, tworzenie nowych miejsc pracy, wartość inwestycji związanych z gospodarką danych. Dzięki takim wskaźnikom administracja będzie mogła podejmować decyzje o dalszych inwestycjach w rozwój infrastruktury danych na podstawie rzeczywistych efektów ekonomicznych. Jednocześnie możliwe stanie się identyfikowanie najbardziej wartościowych zbiorów danych oraz określenie obszarów wymagających poprawy jakości lub częstszej aktualizacji. Realizacja polityki wartości danych publicznych przyniesie korzyści zarówno administracji, jak i przedsiębiorcom oraz obywatelom. Nowoczesne zarządzanie danymi pozwoli zwiększyć efektywność funkcjonowania administracji publicznej, poprawić jakość usług cyfrowych oraz ograniczyć koszty przetwarzania informacji. Jednocześnie rozwój krajowego rynku usług opartych na danych stworzy nowe miejsca pracy dla specjalistów z zakresu informatyki, analityki danych, sztucznej inteligencji i cyberbezpieczeństwa.

- v. Powiązanie suwerenności technologicznej z polityką energetyczną państwa. Dynamiczny rozwój sztucznej inteligencji, chmury obliczeniowej oraz nowoczesnych centrów danych generuje bezprecedensowe zapotrzebowanie na tanią, stabilną i niskoemisyjną energię. Bez zapewnienia takiego zaplecza energetycznego polscy dostawcy technologii stracą konkurencyjność, a koszty utrzymania krytycznych systemów w kraju drastycznie wzrosną. Bezpieczeństwo cyfrowe Polski zależy więc dziś bezpośrednio od tempa transformacji energetycznej, zaś suwerenność technologiczna nie zaistnieje bez zapewnienia odporności i niezależności zasilającej ją infrastruktury.

4. Kontekst taktyczny

Rada ds. Cyfryzacji rekomenduje:

- a. Wybrać 3–4 pilotażowe zamówienia publiczne i przetestować w nich kryteria suwerennościowe (np. jedno zamówienie w obszarze cyberbezpieczeństwa, jedno w obszarze chmury lub danych, jedno w obszarze narzędzi komunikacyjnych dla administracji oraz jedno w obszarze AI lub automatyzacji procesów publicznych).
- b. Przygotować wzorcowe klauzule do SIWZ/SWZ dotyczące zamówień na systemy i usługi ICT, obejmujące w szczególności: interoperacyjność, stosowanie otwartych i powszechnie uznanych standardów, przenoszalność danych i konfiguracji, plan wyjścia (exit plan) oraz możliwość skutecznej zmiany dostawcy lub rozwiązania, audytowalność, wymagania dotyczące lokalizacji i kontroli nad danymi, przeciwdziałanie nieuzasadnionemu uzależnieniu od jednego dostawcy (vendor lock-in), a tam, gdzie jest to uzasadnione – możliwość stosowania modeli wielodostawcowych (dual vendor / multi vendor).

Klauzule powinny również określać wymagania dotyczące dokumentowania i udostępniania interfejsów API, przekazania niezbędnej dokumentacji technicznej oraz zapewnienia możliwości eksportu danych, konfiguracji i innych informacji niezbędnych do migracji lub przejęcia rozwiązania przez innego dostawcę, wraz z odpowiednim wsparciem procesu wyjścia.

Istotnym elementem powinny być także wymagania dotyczące bezpieczeństwa łańcucha dostaw, możliwości jego audytu oraz zapewnienia odpowiedniego wsparcia i aktualizacji bezpieczeństwa w całym wymaganym okresie eksploatacji rozwiązania. Dla wybranych kategorii systemów ICT należy przewidzieć obowiązek dostarczania i aktualizowania SBOM (Software Bill of Materials) w powszechnie stosowanym, maszynowo czytelnym formacie, umożliwiającym identyfikację komponentów oprogramowania i ich zależności oraz wspierającym zarządzanie podatnościami, ryzykiem dostawców i zależnościami technologicznymi.

Zakres i poziom szczegółowości tych wymagań powinny być proporcjonalne do krytyczności systemu, charakteru przetwarzanych danych oraz poziomu ryzyka, ze szczególnym uwzględnieniem systemów administracji publicznej oraz systemów wykorzystywanych przez podmioty kluczowe i ważne.

- c. Uruchomić krajowy katalog rekomendowanych rozwiązań open source i europejskich dostawców dla administracji.
- d. Koordynacja polityki dotyczącej otwartego oprogramowania dla administracji publicznej jak np. ZenDiS (Niemcy), DINUM (Francja) (m.in. zarządzanie kodem finansowanym ze środków publicznych, ograniczanie vendor lock-in, ocena i rekomendacje rozwiązań open source dla samorządów, budowanie kompetencji, wspieranie polskiego sektora ICT).
- e. Repozytorium kodu publicznego dla administracji (jak np. niemiecki openCode)
- f. Katalog minimalnych wymagań dla chmury zaufanej w sektorze publicznym.
- g. Program szkoleń dla zamawiających, m.in. wiedza kupiecka, technologie, negocjacje, licencje, open source, cyberbezpieczeństwo. Można wykorzystać m.in. ścieżki szkoleniowe realizowane przez Urząd Służby Cywilnej.
- h. Stworzenie funduszu kompetencyjnego dla szkół i samorządów przechodzących na otwarte standardy, stworzenie podręczników (guidelines) migracyjnych dla samorządów: poczta, wideokonferencje, komunikacja wewnętrzna, repozytorium dokumentów, backup, cyberhigiena i podstawowe narzędzia open source.
- i. Stworzenie pilotażowej listy kwalifikowanych dostawców lub ramowych umów technologicznych dla administracji, wzorowanych funkcjonalnie na rozwiązaniach typu GSA Schedule, z jasnymi wymaganiami bezpieczeństwa, jakości, audytu i tworzenia wartości w Polsce lub UE.

5. Obszar regulacyjny

Rada ds. Cyfryzacji rekomenduje:

- a. Nowelizację PZP przez dodanie suwerenności technologicznej, interoperacyjności, bezpieczeństwa łańcucha dostaw, otwartych standardów i kosztów wyjścia jako dopuszczalnych kryteriów oceny ofert. Zmiana powinna jednoznacznie wskazać, że kryteria te służą bezpieczeństwu, odporności, interoperacyjności i tworzeniu wartości, a nie automatycznej preferencji narodowościowej.

- b. Wprowadzenie obowiązkowego testu suwerenności technologicznej dla zamówień ICT powyżej określonego progu oraz dla systemów istotnych dla bezpieczeństwa państwa. Test zależności technologicznej powinien być obowiązkowo załączany do dokumentacji dużych zamówień ICT i aktualizowany przy istotnej zmianie architektury, dostawcy, modelu chmurowego lub lokalizacji danych.
- c. Zmianę reguł budżetowych dla dużych projektów cyfrowych. Roczność budżetu powinna być uzupełniona możliwością wieloletniego planowania i finansowania projektów ICT, ponieważ dobre zamówienie technologiczne wymaga analizy rynku, dialogu technicznego, pilotażu, testów bezpieczeństwa i planu migracji.
- d. Wzmocnienie kontroli nad zakupami poza PZP i zakupami spółek Skarbu Państwa (wspólne raportowanie dużych zakupów ICT w trzech strumieniach: PZP, poza-PZP oraz spółki Skarbu Państwa).
- e. Doprecyzowanie partnerstwa publiczno-prywatnego w ICT (należy przygotować bezpieczny model PPP dla projektów cyfrowych, obejmujący własność danych, prawa do kodu, cyberbezpieczeństwo, audyt, exit plan i kontrolę państwa nad komponentami krytycznymi). Model PPP powinien umożliwiać angażowanie kapitału prywatnego w rozwój technologii publicznych, ale bez utraty przez państwo kontroli nad danymi, standardami, architekturą i komponentami krytycznymi.
- f. Wprowadzenie obowiązkowej zasady „public money, public code” – kod tworzony za środki publiczne powinien być co do zasady publikowany na licencji open source, z wyjątkami dla bezpieczeństwa, ochrony informacji niejawnych i krytycznych podatności.
- g. Przygotowanie planu wyjścia z rozwiązań zamkniętych. Każdy duży system publiczny powinien mieć dokumentowany plan migracji, przeniesienia danych i kontynuacji działania w razie zmiany dostawcy.
- h. Przeanalizowanie mechanizmów podatkowych i fiskalnych, które zapewnią, że wartość generowana na polskim rynku cyfrowym będzie w większym stopniu reinwestowana w krajowe kompetencje, infrastrukturę, cyberbezpieczeństwo, AI i transformację cyfrową MŚP.

Podsumowanie

Budowanie suwerenności technologicznej Polski powinno opierać się na kompleksowym podejściu łączącym działania regulacyjne, inwestycyjne i fiskalne. Suwerenność technologiczna nie powinna być rozumiana jako dążenie do izolacji od globalnych rynków, lecz jako zdolność państwa i gospodarki do samodzielnego kształtowania swojego rozwoju cyfrowego, przy jednoczesnym zachowaniu możliwości wyboru, zmiany i współpracy z różnymi dostawcami technologii. Kluczowym warunkiem realizacji tego celu jest zachowanie otwartości technologicznej oraz neutralności technologicznej państwa, umożliwiającej wybór rozwiązań najlepiej odpowiadających potrzebom użytkowników i administracji publicznej. Szczególne znaczenie należy przypisać rozwojowi krajowej i europejskiej infrastruktury cyfrowej, w tym centrów przechowywania i przetwarzania danych, rozwiązań chmurowych oraz sieci nowej generacji, które stanowią fundament odporności państwa i gospodarki na

zagrożenia geopolityczne oraz cybernetyczne. Równolegle niezbędne jest wzmacnianie bezpieczeństwa i odporności cyfrowych łańcuchów dostaw oraz zapewnienie ciągłości działania usług kluczowych dla funkcjonowania państwa i gospodarki.

Jednocześnie konieczne jest tworzenie warunków umożliwiających rozwój polskich i europejskich przedsiębiorstw technologicznych poprzez wspieranie innowacji, badań i rozwoju, komercjalizacji nowych technologii oraz wzmacnianie kompetencji cyfrowych społeczeństwa. Polska powinna aktywnie wspierać rozwój rodzimych rozwiązań technologicznych, aby krajowi i europejscy przedsiębiorcy mogli konkurować nie tylko jako użytkownicy technologii, ale również jako ich twórcy i dostawcy. Szczególne znaczenie powinno zostać przypisane rozwojowi krajowych kompetencji w obszarach strategicznych, takich jak m.in. sztuczna inteligencja, cyberbezpieczeństwo, technologie chmurowe, technologie kwantowe oraz zaawansowana analityka danych, technologie kosmiczne, robotyka.

Istotnym elementem polityki państwa powinno być również ograniczanie nadmiernej zależności od pojedynczych dostawców technologii poprzez wspieranie interoperacyjności systemów, przenoszalności danych oraz rozwiązań umożliwiających swobodną zmianę dostawcy usług cyfrowych. Działania te zwiększają konkurencyjność rynku, wzmacniają bezpieczeństwo użytkowników oraz ograniczają ryzyko technologicznego uzależnienia od podmiotów spoza Unii Europejskiej. Należy również promować stosowanie otwartych standardów, interoperacyjnych rozwiązań technicznych oraz mechanizmów zapobiegających zjawisku vendor lock-in zarówno w sektorze publicznym, jak i prywatnym.

Rada dostrzega również zasadność wprowadzenia podatku rekompensującego od niektórych usług jako jednego z instrumentów wspierających realizację celów związanych z suwerennością technologiczną. Mechanizm ten powinien obejmować wyłącznie największe międzynarodowe platformy cyfrowe, bez względu na kraj pochodzenia, osiągające znaczące przychody na rynku polskim, przy jednoczesnym wyeliminowaniu ryzyka podwójnego opodatkowania oraz nadmiernych obciążeń dla krajowych przedsiębiorców. Wpływy z tego podatku mogłyby zostać przeznaczone na rozwój nowoczesnych technologii wzmacniając fundusz sztucznej inteligencji, wspierając cyberbezpieczeństwo, edukację cyfrową społeczeństwa, rozwój infrastruktury technologicznej oraz krajowe startupy i innowacyjne przedsiębiorstwa. Pożądane byłoby przy tym stworzenie przejrzystych mechanizmów gwarantujących, że środki pozyskane z podatku cyfrowego będą przeznaczane na długoterminowe inwestycje wzmacniające konkurencyjność i odporność cyfrową Polski.

Istotnym elementem budowania suwerenności technologicznej powinno być również zwiększanie kompetencji cyfrowych administracji publicznej oraz wzmacnianie zdolności państwa do skutecznego projektowania, wdrażania i nadzorowania polityk publicznych w obszarze nowych technologii.

Agnieszka Jankowska
Przewodnicząca Rady do Spraw Cyfryzacji
/podpisano elektronicznie/



PODPIS ZAUFANY

**AGNIESZKA
JANKOWSKA**

28.09.2026 23:03:44 GMT+0200

Dokument podpisany elektronicznie
podpisem zaufanym