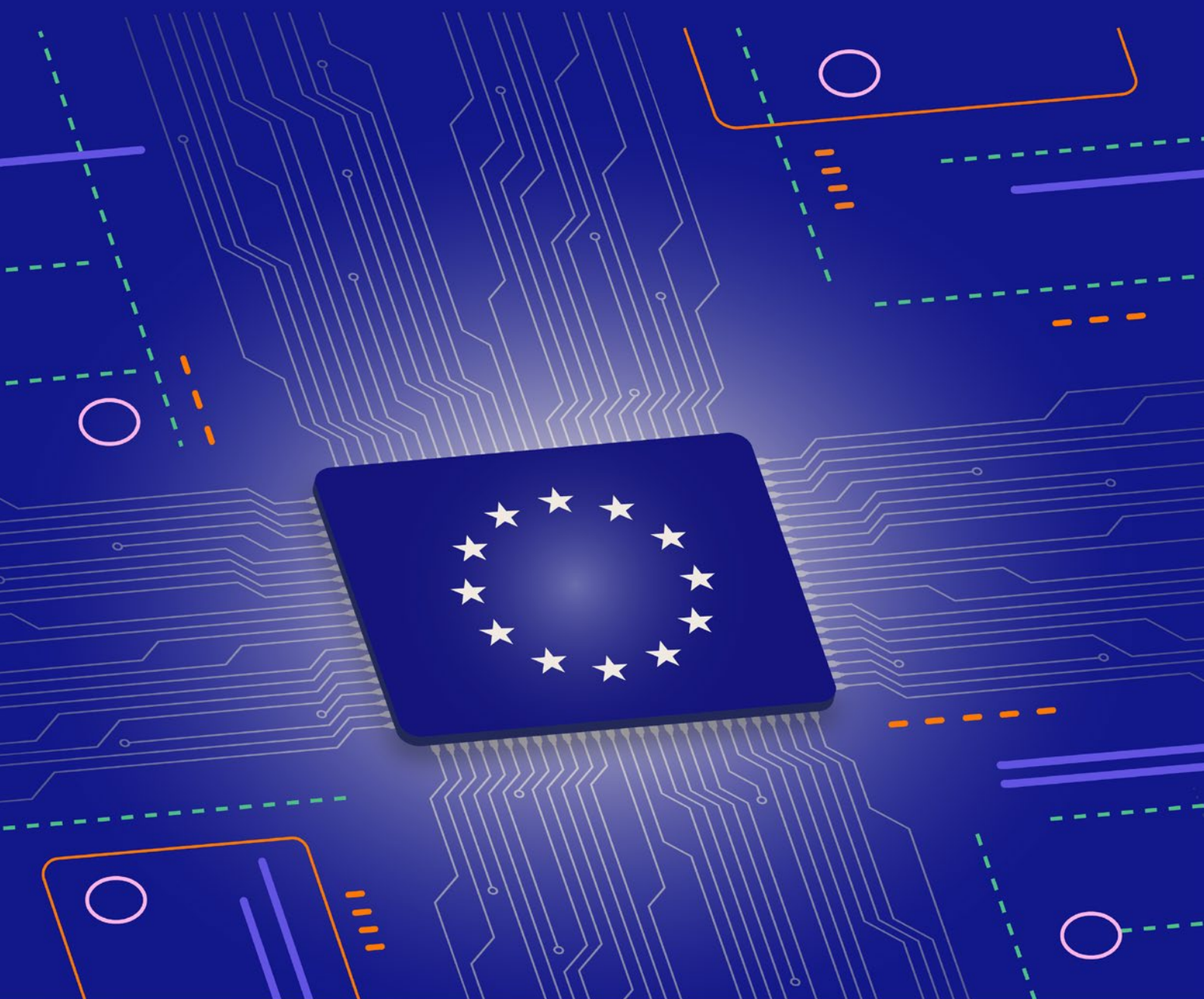


Techsuwerenność Europy

Od idei do praktyki





AUTOR

Jan Jęcz

analityk ds. gospodarki cyfrowej

Polityka Insight

REDAKCJA

Weronika Rędziniak

Polityka Insight

PROJEKT GRAFICZNY

Karolina Tomaszewska

Joanna Pamuła

Polityka Insight

Partnerem raportu jest Orange.

Polityka Insight dołożyła wszelkich starań, by opracowanie było bezstronne i obiektywne. Wszelkie prawa zastrzeżone.



Orange Polska jest jednym z wiodących dostawców usług telekomunikacyjnych w kraju. Posiada największą w Polsce infrastrukturę, dzięki której oferuje usługi w najnowocześniejszych technologiach m.in. internet światłowodowy o prędkości nawet do 8 Gb/s oraz usługi mobilne w technologii 5G. Jest dostawcą kompleksowych rozwiązań dla biznesu, oferuje usługi z zakresu IoT, ICT i cyberbezpieczeństwa. Orange Polska należy do najbardziej zaangażowanych społecznie firm w kraju. Ma jeden z największych programów wolontariatu pracowniczego w Polsce. Poprzez programy Fundacji Orange wspiera edukację cyfrową, ucząc mądrego, bezpiecznego i twórczego korzystania z nowoczesnych technologii.

www.orange.pl

**POLITYKA
INSIGHT**

POLITYKA INSIGHT to źródło wiedzy o polskiej i europejskiej polityce oraz gospodarce dla liderów biznesu, decydentów politycznych i dyplomatów. Od 12 lat dostarcza swoim odbiorcom serwisy analityczne dostępne w abonamentach, przygotowuje raporty i prezentacje na zlecenie polskich i międzynarodowych instytucji oraz organizuje debaty i konferencje. Analitików i analityczki Polityki Insight można usłyszeć w regularnie publikowanych autorskich seriach podcastowych, m.in. Nasłuchu i Energii do zmiany.

www.politykainsight.pl

Warszawa, październik 2025 roku

Spis treści

Kluczowe wnioski	4
Wprowadzenie	6
Część 1. Idea	8
1.1. Jak Europa zwróciła się ku techsuwerenności	8
1.2. Czym jest, a czym nie jest technologiczna suwerenność	10
1.3. Dekada niepokojów: jak Europa zapagnęła techsuwerenności	13
1.4. Czemu służy techsuwerenność	25
Część 2. Praktyka	28
2.1. Stos technologiczny po polsku	28
2.2. Finansowanie techsuwerenności	31
2.3. Techsuwerenność: lekcje ze świata	32
Rekomendacje	38
Bibliografia	40

Kluczowe wnioski

1

Wspólny rdzeń różnych definicji technologicznej suwerenności stanowią dwa elementy: posiadanie możliwości rozwoju technologii oraz swoboda współpracowania w tym zakresie z zewnętrznymi partnerami.

2

Technologiczna suwerenność zawiera w sobie pokrewne rodzaje suwerenności: danych i cyfrową. Jest ściśle powiązana z suwerennością energetyczną, lekową czy żywnościową. Stanowi element europejskiej otwartej autonomii strategicznej, nowej polityki przemysłowej oraz polityki deriskingu. Nie jest natomiast synonimem autarkii ani narodowego protekcjonizmu.

3

W ciągu ostatniej dekady oczekiwania wobec techsuwerenności i stawiane jej cele narastały. Początkowo dotyczyły ochrony prywatności, później także zdolności do regulowania cyfrowych korporacji. Od pandemii techsuwerenność zaczęła być mocniej wiązana z bezpieczeństwem gospodarki, a w kolejnych latach także z jej konkurencyjnością. Dziś rozumiana jest również jako warunek bezpieczeństwa militarnego Europy, a od niedawna – jako fundament jej polityki przemysłowej.

4

Potrzebę technologicznej suwerenności można uzasadnić, spoglądając na nią jako na warunek wykonywania funkcji władzy przez państwa członkowskie i instytucje unijne; niezbędny element do budowy konkurencyjnej gospodarki; wsparcie w transformacji systemowej UE (zielonej, cyfrowej, sprawiedliwej).

5

Popularnym sposobem operacjonalizacji techsuwerenności jest koncepcja europejskiego stosu technologicznego – EuroStacka. Wiele przedsiębiorstw pochodzących z różnych regionów Polski mogłoby już dziś zaangażować się w realizację tej inicjatywy.

6

Wśród możliwych źródeł finansowania europejskiego stosu technologicznego najczęściej wskazywane są trzy niewykluczające się wzajemnie opcje: zamówienia publiczne priorytetyzujące europejskie spółki; mobilizacja środków z unijnego rynku kapitałowego; fundusze w ramach unijnego budżetu na lata 2028-2034.

7

Oprócz uczenia się od siebie nawzajem, kraje członkowskie Unii Europejskiej powinny też zwrócić uwagę na lekcje płynące z techsuwerennościowych dążeń państw w innych regionach świata, w szczególności Stanów Zjednoczonych, Chin, Indii, Brazylii, Tajwanu.

Wprowadzenie

„Suwerenność” to w Europie i w Polsce technologiczne słowo 2025 roku. Nie będzie przesadą stwierdzenie, że w ostatnich miesiącach mówią o niej wszyscy: politycy i urzędnicy, przedstawiciele biznesu, organizacje pozarządowe, akademicy, media. Rozmowy toczą się w każdym z sektorów gospodarki związanych z nowymi technologiami: nie tylko w teleinformatyce (ICT), lecz także w sektorach kosmicznym, obronnym, motoryzacyjnym, energetycznym, farmaceutycznym, biotechnologicznym i wielu innych.

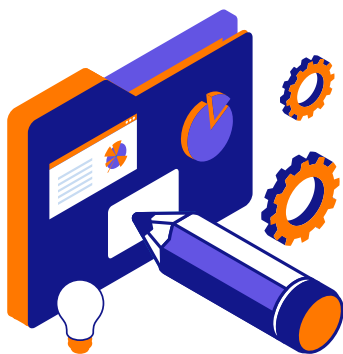
Czym jest techsuwerenność? To pojęcie wieloznaczne. Według jednej z najpowszechniej stosowanych definicji stanowi ona „**zdolność do generowania wiedzy naukowo-technicznej w sposób autonomiczny lub pozyskiwania do niej dostępu w ramach stabilnych partnerstw bez ograniczeń**”¹. Te dwa elementy – posiadanie możliwości rozwoju technologii (poprzez badania i rozwój czy produkcję) oraz swoboda współpracowania w tym zakresie z zewnętrznymi partnerami – łączą większość rozumień tego pojęcia.

By podnieść poziom świadomości, jak złożoną ideą jest techsuwerenność, w pierwszej części raportu opisuje jej korzenie oraz kontekst, w którym się rozwija. Obecne wzmożenie wokół uniezależniania się Wspólnoty Europejskiej od dostawców produktów i usług z państw trzecich nie wzięło się znikąd. Bezpośrednio wywołał je kryzys relacji transatlantyckich, spowodowany polityką zagraniczną Donalda Trumpa na starcie jego drugiej kadencji. Jednak to, że dominującą reakcją na ten wstrząs był zwrot ku idei suwerenności, nie zaś na przykład apele, by przyjmując żądania Ameryki, było skutkiem trwających od lat procesów społecznych, gospodarczych i dyskursywnych. Raport ten ma je odsłonić. Jednocześnie, mimo powszechnie deklarowanego poparcia dla suwerenności technologicznej, po bliższym zbadaniu często okazuje się, że różne osoby i środowiska rozumieją ją na różne sposoby. Niejednoznaczność pojęcia bywa wykorzystywana do atakowania samej idei. Posiłkując się literaturą akademicką, niniejsza praca ma w przystępny sposób uporządkować pole semantyczne, ułatwiając prowadzenie rozmów o techsuwerenności.

Raport porządkuje także cele uniezależniania się w obszarze nowych technologii, przede wszystkim związane z bezpieczeństwem. Suwerenność nie jest europejską zachcianką, kosztownym przedsięwzięciem bez praktycznych zastosowań, lecz środkiem mogącym wspomóc realizację kluczowych planów, jak podnoszenie bezpieczeństwa wewnętrznego i zewnętrznego czy podwójna (zielona i cyfrowa) transformacja. Przekonujące opowiedzenie mierzalnych korzyści jest istotne choćby po to, by prosuwerennościowe wysiłki miały społeczne poparcie.

Głównym wątkiem dyskusji o suwerenności technologicznej jest poszukiwanie odpowiedzi na pytanie, jak zwiększyć niezależność kontynentalnej wspólnoty. Różne środowiska proponują odmienne plany, częściowo się zazębiające, lecz w wielu kwestiach sporne. Różnice dotyczą choćby finansowania: czy powinno opierać się raczej na wielkoskalowych inwestycjach z unijnego budżetu, czy też nacisk powinno się kłaść na zamówienia publiczne od europejskich podmiotów. Sporną kwestią jest, czy dążenia suwerennościowe wymagają upraszczania, czy wręcz eliminowania konkretnych regulacji. Ważnym pytaniem jest też to o technologiczne priorytety. Czy prym powinna wieść sztuczna inteligencja, czy może usługi chmurowe? Podobnych problemów, składających się na pytanie „jak”, jest wiele.

W części raportu zatytułowanej „Praktyka” znajdują się zmapowane pomysły na to, jakimi środkami Europa i Polska mogą dążyć do technologicznej suwerenności. Ambicją tego dokumentu nie jest jednak rozstrzygnięcie sporów o metodę. W tym duchu służy on opisaniu skali wyzwań i wskazaniu obecnych w debacie pomysłów na rozwiązania. Zawiera również zestaw kluczowych rekomendacji istotnych do uwzględnienia w decyzjach strategicznych, regulacyjnych i gospodarczych.



Część 1.

Idea

1.1. Jak Europa zwróciła się ku techsuwerenności

Jedną z pierwszych prac naukowych poświęconych technologicznej suwerenności jest artykuł Paula Granta z 1983 roku o wdzięcznym tytule *Technological sovereignty: forgotten factor in the 'hi-tech' razzamatazz*. Choć powstała w zupełnie odmiennym kontekście historycznym i geograficznym od współczesnego, europejskiego, to pokazuje, jak niewiele zmieniła się debata. Grant krytykował w swojej pracy władze Australii za to, że jako jedyny spośród „drugorzędnych krajów uprzemysłowionych” nie stara się osiągnąć technologicznej suwerenności². Pojęcie to definiował jako „**zdolność i wolność do wybierania, generowania lub nabywania oraz stosowania, rozwijania i wykorzystywania komercyjnie technologii niezbędnych innowacjom przemysłowym**”³. Wśród omawianych przez niego mechanizmów poprawy suwerenności Australii można znaleźć między innymi preferencyjne traktowanie lokalnych firm w zamówieniach publicznych oraz inwestycje w wielkoskalowe projekty o znaczeniu strategicznym⁴.

40 lat później po drugiej stronie globu trwają intensywne rozmowy, w których pobrzmiewają te same obawy i proponowane są bliźniacze rozwiązania. Podobne jest też dominujące rozumienie technologicznej suwerenności. **Gdy w 2020 roku Ursula von der Leyen w felietonie dla europejskiej prasy definiowała „techsuwerenność” Unii, kładła akcent na posiadanie zdolności technologicznych oraz swobodę podejmowania wyborów co do technologii (na przykład w ramach współpracy międzynarodowej)**⁵. Podobne rozumienie, które opiera się na dwóch filarach – własnych kompetencjach i swobodzie kształtowania relacji z zewnętrznymi podmiotami – dominuje współcześnie w literaturze akademickiej oraz dokumentach strategicznych⁶.

Przez 40 lat od publikacji pracy Granta, szczególnie zaś w ciągu ostatniej dekady, radykalnie zmienił się jednak kontekst rozmów. **Przewrót w myśleniu o suwerenności spowodowała przede wszystkim tzw. czwarta rewolucja przemysłowa**. W efekcie wzrostu znaczenia digitalizacji jako jednego z kluczowych procesów społecznych i gospodarczych, epitet „cyfrowa” zaczął zastępować określenie „technologiczna” w debacie o suwerenności, stając się z czasem jego synonimem. Sygnalizowało to zmianę priorytetów Europy. Najważniejsza stała się budowa zdolności w obszarach infrastruktury i usług chmurowych czy sztucznej inteligencji, by uniezależnić się tak od tradycyjnych rywali, jak i handlowych partnerów. W procesie technologicznej rewolucji wykształciła się też nowa kategoria podmiotów: globalne korporacje cyfrowe popularnie zwane big techami. Postrzegane początkowo przez pryzmat techno- optymizmu jako przyjaźni partnerzy sektora publicznego, prywatnego, mediów czy NGO, z czasem zaczęły być uważane również za źródło zagrożeń. Medialne skandale z udziałem tych przedsiębiorstw⁷, a także pojawiające

W procesie technologicznej rewolucji wykształciła się też nowa kategoria podmiotów: globalne korporacje cyfrowe, popularnie zwane big techami.

się z biegiem lat obszerne analizy krytyczne ich modeli biznesowych, opartych na inwigilacji i uspołecznianiu kosztów⁸, wywołały lawinę wątpliwości co do zakresu ich rzeczywistego wpływu na politykę, gospodarkę i społeczeństwo.

Kryzys globalizacji i wolnego handlu to kolejna ważna zmiana, która nadała nowy kontekst dyskusjom o suwerenności technologicznej w Europie w ostatnich latach.

Coraz otwarciej mówi się o tym, że „wiele krajów zaczęło (...) agresywnie kwestionować ramy instytucjonalne leżące u podstaw wolnego handlu i uczciwej konkurencji, które przez dziesięciolecia były uważane za coś oczywistego”⁹. Przez długi czas zarzuty te w Europie kierowano przede wszystkim względem

Chin. Agresywna, protekcyjnistyczna polityka handlowa Pekinu w obszarach motoryzacji czy e-handlu wywoływała w Europie niepokój. Jednocześnie doświadczenia pierwszej kadencji Donalda Trumpa powodowały obawy, że za pewnik nie należy brać nawet siły relacji transatlantycznych. Potwierdziły się one w pełni w drugiej kadencji amerykańskiego prezydenta. Jednak nie tylko niepokój wywołany konfliktami handlowymi powodował zwrot w myśleniu Brukseli i europejskich stolic o roli władzy publicznej w gospodarce. Inne podstawy dryfu w polityce przemysłowej Europy – od kreowania rynku do kierowania rynkiem – to między innymi obawy o pozostawanie w tyle w globalnym wyścigu gospodarczym czy potrzeba znalezienia nowej narracji dla unijnej integracji¹⁰.

Wyliczając procesy o skali zdolnej zmienić paradygmat, które uformowały debatę o suwerenności technologicznej, nie sposób nie wspomnieć o wzroście obaw o bezpieczeństwo Europy. Niektórzy badacze twierdzą wręcz, że „[p]ojęcie suwerenności technologicznej nie może zostać oderwane od koncepcji bezpieczeństwa”¹¹. Związki między nimi istnieją we wszystkich wymiarach bezpieczeństwa, niezależnie od przyjętej typologii: trójdzielnej stosowanej przez OBWE (wymiar polityczno-wojskowy, ekonomiczno-środowiskowy i ludzki)¹² czy siedmiowymiarowej, którą posługiwała się Polska w czasie prezydentury w Radzie Unii Europejskiej (wymiar zewnętrzny, wewnętrzny, informacyjny, ekonomiczny, energetyczny, żywnościowy, zdrowotny).

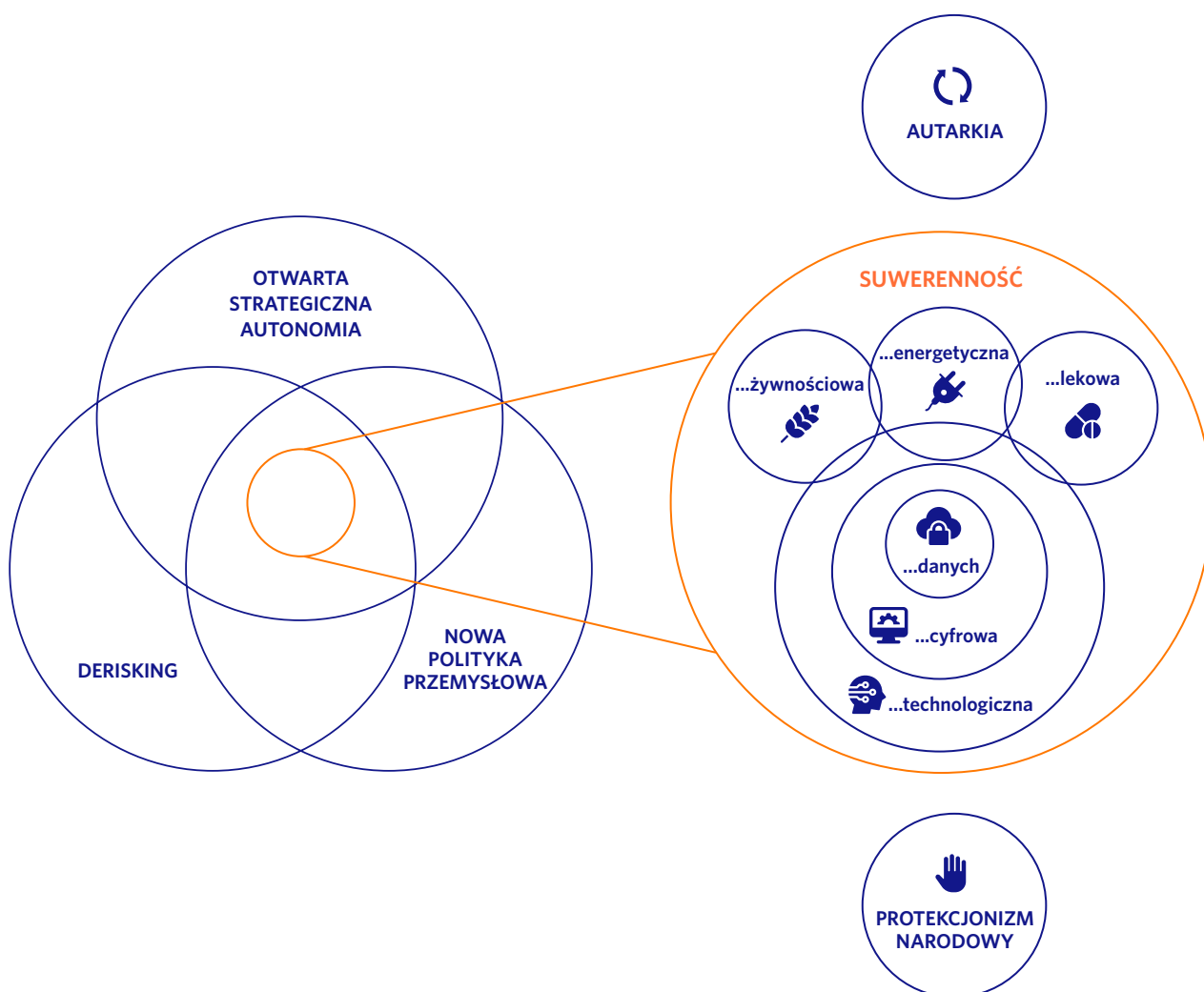
W ostatnich latach relacje między suwerennością technologiczną a ładem w Europie stały się oczywiste szczególnie w świetle dwóch kryzysów: pandemii COVID-19 i jej następstw, a także pełnoskalowej inwazji Rosji na Ukrainę oraz nasilenia rosyjskiej wojny hybrydowej w Europie¹³.

Kryzys energetyczny jasno pokazał też krytyczne znaczenie potrzeby zwiększania niezależności w obszarach gospodarki, od których zależy funkcjonowanie całego państwa. Wstrząsy te na różne sposoby dały argumenty za tezą, że zmniejszanie zależności UE od zewnętrznych aktorów w obszarze nowych technologii (od badań i rozwoju po dostęp do gotowych usług i produktów) zwiększy odporność wspólnoty.

1.2. Czym jest, a czym nie jest technologiczna suwerenność

Debata na temat techsuwerenności powiązana jest z dyskusjami toczącymi się wokół towarzyszących konceptów teoretycznych. Na podstawie przeglądu literatury można podzielić je na kilka kategorii: synonimy o węższym i szerszym znaczeniu, pojęcia częściowo pokrywające się znaczeniowo oraz te rozbieżne, choć łączone z techsuwerennością. Relacje te ilustruje poniższy diagram.

ZALEŻNOŚCI POMIĘDZY POJĘCIEM TECHSUWERENNOŚCI I POKREWNymi



ŹRÓDŁO: OPRACOWANIE WŁASNE.

Omawiając te zależności, należy na wstępie zaznaczyć, że suwerenność technologiczna powiązana jest z innymi pojęciami dotyczącymi **suwerenności w różnych obszarach gospodarki: energetyce, produkcji leków czy żywności. Każdy z nich zawiera w sobie istotny komponent technologiczny, ale niekoniecznie jest do niego sprowadzalny.** Zakres, w jakim pojęcia się pokrywają, jest różny – w pewnych kontekstach mogą jednak stanowić synonimy¹⁴. Co do zasady raport ten przyjmuje jednak, że suwerenność technologiczna nie jest tożsama z suwerennością w określonych gałęziach przemysłu wysokich technologii.

Pojęcia **suwerenność cyfrowa i danych** to, podobnie jak suwerenność technologiczna, terminy wieloznaczne, bez ustalonej definicji, rozumiane różnie w zależności od retorycznych potrzeb. W uproszczeniu stanowią odpowiednio mniejsze podkategorie techsuwerenności. **Suwerenność danych zawiera się w cyfrowej, która z kolei zawiera się w technologicznej.** Deficytowy rdzeń pojęcia *digital sovereignty* stanowi idea „kontroli tego, co cyfrowe w warstwie fizycznej (zasoby, infrastruktura, urządzenia), warstwie kodu (standardy, zasady, design) oraz w warstwie informacji (treści, dane). Kontrola oznacza zdolność, by wpływać na oraz ograniczać produkcję (w tym wydobywania i przetwarzania niezbędnych surowców), projektowanie, wykorzystanie wyników technologii cyfrowych”¹⁵. Jak wynika z tej definicji, suwerenność danych odnosi się głównie do warstwy informacji. Pojęcie to odnosi się także do kontroli i „[w]ystępuje przede wszystkim w kontekście debat dotyczących projektowania architektury IT i/lub przepisów mających zastosowanie do przetwarzania danych (...)”¹⁶. Ze względu na gospodarcze znaczenie danych i infrastruktury do ich przechowywania oraz przetwarzania (przede wszystkim chmury), ten rodzaj suwerenności stanowi zdaniem niektórych autorów fundamentalny warunek niezależności technologicznej w ogóle¹⁷.

Otwarta strategiczna autonomia (OSA) to nowe podejście do polityki handlowej, które wykształciło się w Unii Europejskiej w reakcji na pandemię COVID-19. Komisja Europejska definiuje je jako obejmujące „odporność i konkurencyjność, aby wzmocnić gospodarkę UE; zrównoważony rozwój i sprawiedliwość odzwierciedlające potrzebę odpowiedzialnego i sprawiedliwego działania UE; asertywność i współpracę opartą na zasadach, aby pokazać preferencje UE w zakresie współpracy międzynarodowej i dialogu, a także jej gotowość do zwalczania nieuczciwych praktyk i stosowania w razie potrzeby niezależnych narzędzi w celu realizacji swoich interesów”¹⁸. Choć pojęcie to wprowadzone zostało przy okazji przeglądu polityki handlowej, odnosi się także do polityki przemysłowej Unii Europejskiej. **OSA opiera się na założeniu, że rozwój wolnego handlu musi iść w parze z interwencjami w wewnętrzny rynek mającymi uczynić europejską gospodarkę bardziej konkurencyjną, odporną na wstrząsy, rozwijającą się w sposób zrównoważony. Tworzy to napięcia, w których centrum znajduje się suwerenność technologiczna.** Zabiegi o uniezależnienie się Europy od państw trzecich w obszarze nowych technologii mogą ograniczać pełną otwartość handlu czy wolnorynkową konkurencję¹⁹, na przykład poprzez bariery stawiane tzw. dostawcom wysokiego ryzyka czy preferencyjne traktowanie europejskich podmiotów w zamówieniach publicznych. Co do zasady techsuwerenność wpisuje się w politykę OSA, stanowiąc narzędzie jej realizacji²⁰.

Nowa polityka przemysłowa to określenie stosowane w literaturze naukowej i publicystyce na zmianę paradygmatu w myśleniu o gospodarce, obserwowaną w Europie mniej więcej od połowy drugiej dekady XXI wieku²¹. Jej wyrazem była zaktualizowana w 2021 roku strategia przemysłowa UE²², jednak koncepcja ta wykracza poza opisane w dokumencie działania. **Charakteryzuje ją przede wszystkim odejście od leseferyzmu i ograniczenia roli administracji do wyłącznie kreatora rynków, które same dostarczają produkty i usługi niezbędne do realizacji funkcji państwa, w kierunku interwencjonizmu i kierowania rynkiem, gdy jest niewydolny.** Przyjęcie polityki OSA to jeden z przejawów transformacji w myśleniu o gospodarce. Innym terminem pomagającym zrozumieć nową politykę przemysłową jest geo-dirigizm: „pogląd, że rynki pozostawione same sobie nie zapewnią wystarczających kompetencji technologicznych i konkurencyjności gospodarczej niezbędnych do przetrwania i prosperowania w (...) świecie, w którym technologia i geopolityka są coraz bardziej ze sobą powiązane”²³.

Między technologiczną suwerennością a międzynarodowym handlem i współpracą istnieje (...) dwustronna relacja.

Z tej perspektywy **suwerenność technologiczna/cyfrowa stała się sztandarem, pod którym Komisja Europejska stara się w ostatnich latach organizować poparcie dla nowej polityki przemysłowej**²⁴.

Wśród powiązanych z pojęciem techsuwerenności konceptów dotyczących unijnej polityki warto wskazać także **derisking**. Dotyczy on ograniczania ryzyka wynikającego z uzależnienia gospodarczego od państw trzecich, jednak bez zrywania z nimi relacji (*decoupling*). Podejście to wykształciło się w 2023 roku, a jego najpełniejszy wyraz stanowi przyjęta wówczas europejska strategia bezpieczeństwa gospodarczego²⁵.

Początkowo derisking dotyczył głównie relacji UE-Chiny, stanowiąc odpowiedź Europy na amerykańską politykę decouplingu od Pekinu. W ostatnich miesiącach coraz częściej przywołuje się ten termin także w kontekście relacji transatlantyckich²⁶. Technologiczna suwerenność, obok między innymi uniezależniania się w obszarze energetyki, stanowi jeden z rdzeni polityki deriskingu. Klasyczny przykład, wskazywany w europejskiej strategii gospodarczej, to problem ochrony infrastruktury cyfrowej, zwłaszcza sieci 5G²⁷. W praktyce oznacza to między innymi wprowadzenie mechanizmów umożliwiających ograniczanie lub wykluczanie z prac nad jej rozwojem określonych dostawców sprzętu i usług. Tego rodzaju punktowe interwencje oparte na analizie ryzyka są esencją deriskingu.

A czym techsuwerenność nie jest, choć pozornie może się wydawać? Po pierwsze nie jest marzeniem o **autarkii**²⁸, gdyż „[z]dolność do pojmowania, rozwijania lub wytwarzania nowych technologii nie może być mylona z próbą faktycznego robienia tego wszystkiego we wszystkich kluczowych technologiach wspomagających i/lub ich komponentach”²⁹. Polityka otwartej, strategicznej autonomii nie bez przyczyny ma w nazwie otwartość. Niektórzy analitycy piszą w tym kontekście o „szlachetnym cyklu” otwartości i budowania politycznej oraz ekonomicznej siły: „[i]m silniejsza jest UE pod względem technologicznym i gospodarczym, tym większą ma siłę przebicia w międzynarodowych negocjacjach i stosunkach handlowych; a im bardziej jest otwarta na międzynarodową współpracę i relacje, tym większą siłę gospodarczą i autonomię może osiągnąć”³⁰. Między technologiczną suwerennością a międzynarodowym handlem i współpracą istnieje więc dwustronna relacja. W jedną stronę opiera się na tworzeniu przewag konkurencyjnych, redukowaniu asymetrii informacji oraz rozwijaniu zdolności absorpcji technologii. W drugą stronę międzynarodowy handel wspiera techsuwerenność, zwiększając rozmiar globalnego rynku, kreując konkurencję i zachęty do innowacji, a także prowadząc do większej efektywności prac badawczo-rozwojowych³¹.

Technologiczna suwerenność nie jest też wezwaniem do **narodowego protekcjonizmu**. Stosowanie takiej polityki wobec lokalnych przedsiębiorstw przez państwa członkowskie może wręcz pogrzebać cały projekt. Żaden europejski kraj nie jest w stanie samodzielnie rozwijać zdolności badawczo-rozwojowych czy produkcyjnych umożliwiających wejście w rywalizację z USA i Chinami. W 2020 r. autorzy raportu *Technology sovereignty. From demand to concept* przestrzegali przed tym rząd w Berlinie, pisząc: „[d]la Niemiec, biorąc pod uwagę zakres wzajemnych zależności gospodarczych i politycznych oraz wartość dodaną, jaką zapewniają one dzięki korzyściom wynikającym ze specjalizacji i stabilności

politycznej, punktem odniesienia dla suwerenności technologicznej jest zdecydowanie UE. Odruch renacjonalizacji w obliczu dążenia do suwerenności technologicznej byłby nie tylko nieefektywny, ale w dłuższej perspektywie nawet szkodliwy, ponieważ wywołałby spiralę protekcjonizmu³². Jednocześnie niemożliwe wydaje się prowadzenie debaty o techsuwerenności bez odnoszenia się do protekcjonizmu – nie jako strategii dla Europy, ale zagrożenia. Chiny i USA, szczególnie po zmianie władzy w Białym Domu, otwarcie angażują się w tego rodzaju politykę. Chroniąc swoje interesy, UE mierzy się więc nieustannie z pytaniem, na ile działa w „obronie koniecznej”, a kiedy przekracza jej granice. Zarzut bycia narzędziem protekcjonistycznej polityki stawiany jest choćby unijnemu instrumentowi przeciwko wymuszeniu ekonomicznemu³³. Powstały jako sposób ochrony przed presją Pekinu, w ostatnich miesiącach rozważany był jako broń w potencjalnej wojnie handlowej z Waszyngtonem.

1.3. Dekada niepokojów: jak Europa zapragnęła techsuwerenności

Mając zarysowane tło w postaci ogólnych kontekstów i otoczenia semantycznego technologicznej suwerenności, można przejść do bardziej szczegółowego opisu rozwoju tej idei. Prezentowana poniżej analiza skupia się na kluczowych kontekstach, w jakich techsuwerenność dyskutowana była w literaturze akademickiej i raportach eksperckich, unijnych i polskich dokumentach rządowych, jak również w wypowiedziach europejskich polityków. **Ten historyczny przegląd ma pokazać, że apele o uniezależnianie się w obszarze technologii nie są chwilową modą, oraz że idea ta odpowiada na szeroki wachlarz problemów.**

Podrozdział uporządkowany jest chronologicznie według kluczowych wydarzeń, które uruchamiały w Europie dyskusje o techsuwerenności. Jednocześnie każdy z wątków omawiany jest zgodnie z własną osią czasu, toteż zwykle jedna sekcja kończy się opisaniem wydarzeń późniejszych od otwierających następną.



2013: POCZĄTEK OBAW O PRYWATNOŚĆ DANYCH EUROPEJCZYKÓW

W 2013 roku ujawnione zostały doniesienia sygnalisty Edwarda Snowdena o globalnych naruszeniach prywatności przez administrację USA. Wywołały one dyskusję o tym, czy korzystanie z usług amerykańskich przedsiębiorstw technologicznych jest do pogodzenia z ochroną prywatności danych. Ujawnione przez niego dokumenty opisywały program wielkoskalowej inwigilacji prowadzony przez amerykańską National Security Agency, w którym uczestniczyły firmy dostarczające cyfrowe usługi czy hardware³⁴.

Już w 2015 roku podczas konferencji NATO o cyberkonfliktach Tim Maurer i zespół wskazywali to wydarzenie jako punkt zapalny zwrotu ku technologicznej suwerenności w Europie. W swojej analizie badacze zidentyfikowali szereg technicznych i pozatechnicznych propozycji zwiększenia bezpieczeństwa danych z ponad 12 państw UE, wyróżniając Niemcy jako kraj przewodzący tym staraniom. Pomysły dotyczyły zarówno legislacji, jak nowa dyrektywa ws. ochrony danych; standaryzacji, na przykład wymogu przechowywania określonych danych w centrach na terenie Europy; czy międzynarodowych inwestycji w infrastrukturę pokroju kabli podmorskich.

Stany Zjednoczone nie są oczywiście jedynym państwem trzecim, które nie cieszy się pełnym zaufaniem UE w obszarze bezpieczeństwa danych. Najwięcej obaw dotyczy przede wszystkim administracji Chin sprawującej de facto kontrolę nad danymi gromadzonymi przez krajowe spółki, w Europie aktywne choćby w branżach e-handlu i mediów społecznościowych³⁵. Na niektórych europejskich rynkach – w Holandii, Niemczech czy Irlandii – istotną rolę odgrywają też chińscy hiperskalerzy (najwięksi dostawcy usług chmurowych)³⁶. **Słabnące zaufanie do firm z USA jest jednak szczególnym wyzwaniem, zważywszy na poziom uzależnienia Europy od ich usług.** Według Synergy Research Group w pierwszej połowie 2025 roku Amazon, Microsoft i Google odpowiadały za ok. 70 proc. całego rynku usług chmurowych w Europie³⁷.

Najważniejszym skutkiem tzw. afery Snowdena w Unii Europejskiej było uchwalenie ogólnego rozporządzenia o ochronie danych³⁸. RODO nie było jednak panaceum na problemy z cyfrową prywatnością Europejczyków. W wymiarze transatlantyckim miały ją wzmocnić nowe ramowe zasady transferu danych. Poprzednie porozumienie o nazwie *Safe Harbor Principles*, które obowiązywało w momencie ujawnienia rewelacji Snowdena, zostało unieważnione przez Trybunał Sprawiedliwości Unii Europejskiej wyrokiem Schrems I. Nazwa ta pochodzi od nazwiska Maksa Schremsa, inicjatora postępowania, który zaskarżył również nowe, zawarte w 2016 roku porozumienie UE z USA *Privacy Shield*. Ono również zostało przez TSUE uznane – wyrokiem Schrems II z 2020 roku – za wadliwe jako niezapewniające odpowiedniego poziomu ochrony danych osobowych.

RODO nie było
jednak panaceum
na problemy
z cyfrową
prywatnością
Europejczyków.

W 2022 roku UE i USA ustaliły nowe zasady, tzw. *Data Privacy Framework*. We wrześniu 2025 roku Sąd Pierwszej Instancji uznał ich legalność³⁹. Mimo to ich przyszłość pozostaje niepewna, zważywszy na możliwość apelacji do TSUE. Taki krok rozważa między innymi założone przez Schremsa NGO noyb, którego zdaniem postępująca erozja państwa prawa w Stanach Zjednoczonych wpływa na nielegalność porozumienia⁴⁰. Niezależnie od tego, co stanie się z *Data Privacy Framework*, USA trudno będzie odzyskać raz utracone zaufanie. Amerykańskie firmy świadczące w UE usługi związane z przechowywaniem, transferem

i przetwarzaniem danych starają się uspokoić obawy, oferując „suwerenne” rozwiązania⁴¹. Choć są one interesujące w detalach dotyczących na przykład szyfrowania, w większości przypadków nie rozwiązują podstawowego problemu, który wynika z faktu, że amerykańskie firmy podlegają amerykańskiemu prawu.



Ta niepewność coraz silniej skłania przedstawicieli sektora publicznego, by powierzać dane wyłącznie lokalnym podmiotom, które podlegają w całości tylko europejskiej jurysdykcji. Szacunki Synergy Research Group przewidują wzrost przychodów europejskich dostawców usług chmurowych w 2025 roku o 24 proc. w ujęciu rocznym. Według analityków firmy napędza go przede wszystkim sprzedaż usług w modelu *Infrastructure as a Service* i *Platform as a Service* sektorowi publicznemu⁴². Suwerenne zdolności przetwarzania danych w Unii ma też poprawić między innymi regulacja *Cloud and AI Development Act*, której konsultacje zakończyły się w lipcu 2025 roku.



2018: POCZĄTEK TECHLASHU I NARODZINY CYFROWEGO KONSTYTUCJONALIZMU

Afera Snowdena i wywołane nią obawy o bezpieczeństwo cyfrowych danych Europejczyków były szokiem o ograniczonym zasięgu. Choć bez wątpienia sprawa przebiła się do powszechnej świadomości, nie zdołała naruszyć dominującego na świecie technooptymizmu. Korzyści, jakie biznes i społeczeństwo odczuwały z rozwoju cyfrowych platform – w postaci darmowej rozrywki, narzędzi do komunikacji i zrzeszania się, prowadzenia sprzedaży usług i produktów oraz marketingu na masową skalę – przeważały nad nielicznymi jeszcze wówczas ostrzeżeniami ekspertów⁴³.

Sytuację diametralnie zmieniły informacje ujawnione w 2018 roku przez sygnalistę Christophera Wyliego. Skandal znany pod nazwą **Facebook-Cambridge Analytica** uświadomił społeczeństwu i rządzącym nie tylko to, z jaką łatwością cyfrowe korporacje gromadzą i jak niefrasobliwie traktują dane o swoich użytkownikach. Dotyczył przede wszystkim niebezpieczeństwa wykorzystania tych danych do manipulacji procesami demokratycznymi.

Kilka miesięcy po ujawnieniu sprawy oraz po serii pomniejszych afer związanych z rosnącą presją na big techy, by wzięły odpowiedzialność za społeczne koszty swojej działalności, Rana Foroohar na łamach „Financial Times” ogłosiła techlash słowem roku. Ta zbitka słów tech i backlash oznacza „[r]osnącą niechęć opinii publicznej wobec dużych firm technologicznych z Doliny Krzemowej i ich chińskich odpowiedników”. „Techlash” – pisała Foroohar – „jest przewidywalnym następstwem sytuacji, w której branża nie potrafi sama sobą zarządzać. Nic dziwnego, że nawet osoby z wewnątrz, takie jak Tim Cook z Apple, domagają się obecnie uregulowania sektora”⁴⁴.

Unia Europejska odpowiedziała na te apele. Jednym z elementów cyfrowej agendy dla nowej Komisji Europejskiej, zaproponowanej w 2019 przez Ursulę von der Leyen, był akt o usługach cyfrowych (DSA). Miał on „uaktualnić (...) zasady dotyczące odpowiedzialności i bezpieczeństwa w odniesieniu do platform cyfrowych, usług i produktów”⁴⁵. Zapowiedź tej regulacji w manifestie von der Leyen była świadectwem, że – dzięki staraniom środowisk podnoszących przez lata potrzebę zajęcia się kosztami nieuregulowanego rozwoju cyfrowego kapitalizmu – *techlash* wszedł do głównego nurtu.

Należy przy tym zaznaczyć, że **istotnym kontekstem ewolucji europejskiego prawa była ekspansja chińskich platform: społecznościowych oraz e-handlu**. TikTok pojawił się w Europie w połowie 2018 roku, zaczynając dzięki przejęciu serwisu musica.ly z ogromną bazą użytkowników. Już trzy lata później praktyki spółki dotyczące transferów danych stały się przedmiotem postępowania irlandzkiego regulatora. W maju 2025 roku zakończyło się ono karą w wysokości 530 milionów euro⁴⁶. Zarówno TikTok, jak i platformy zakupowe AliExpress i Shein urosły znacząco w okresie pandemii. Równolegle rosły obawy, że słaba weryfikacja sprzedawców w obu serwisach doprowadzi do zalania Europy niebezpiecznymi produktami. Wszystko to nie uszło uwadze regulatorów pracujących już wówczas nad nowymi rozporządzeniami.

Nowa Komisja przedstawiła DSA w pakiecie z aktem o rynkach cyfrowych (DMA). Pierwszy dotyczy przede wszystkim ochrony konsumenckiej użytkowników wielkich platform. Drugi stanowi regulację antymonopolową, adresującą problem nierównego pola gry na rynku cyfrowym. Oba akty zostały przyjęte w 2022 roku, stając się filarem nowego podejścia UE do regulowania cyfrowej gospodarki: cyfrowego konstytucjonalizmu⁴⁷. Zastąpił on dominujący wcześniej model sędziowskiego aktywizmu, w którym zasady funkcjonowania w cyfrowej gospodarce były wyznaczane przez kolejne orzeczenia TSUE. **„Cyfrowe konstytucje” w postaci DSA i DMA przeniosły ciężar odpowiedzialności za regulowanie platform z europejskiej judykatury na legislaturę i egzekutywę, stanowiąc krok milowy w dążeniach Europy do technologicznej suwerenności.** Wyznaczyły kurs, którym Europa podąża, pracując nad kolejnymi cyfrowymi aktami.



2019: PIERWSZE PODATKI CYFROWE W EUROPIE

Równolegle do prac nad przepisami chroniącymi usługobiorców i rynkowych konkurentów cyfrowych przedsiębiorstw toczyły się dyskusje nad opodatkowaniem tych firm. Formalny dialog w UE ws. podatków cyfrowych zainicjowany został podczas szczytu cyfrowego w Tallinie w 2017 roku. Wśród jego konkluzji znalazło się wezwanie do utworzenia „skutecznego i sprawiedliwego systemu podatkowego na miarę ery cyfrowej” wraz z postulatem, by Komisja Europejska przedstawiła propozycję w tym zakresie⁴⁸. Kilka miesięcy później organ wywiązał się z tego zadania dwoma projektami dyrektyw⁴⁹. Spotkały się one jednak ze sprzeciwem Irlandii, Danii i Szwecji. Protest przyczynił się do tego, że plan europejskiego podatku od usług cyfrowych (DST) porzucono na rzecz zaangażowania się w prace nad reformą podatkową na poziomie OECD⁵⁰.

Choć Bruksela porzuciła ambicje wprowadzenia nowej daniny, sam pomysł nie umarł – przeniósł się na poziom państw członkowskich. Opodatkowanie cyfrowych gigantów zaczęło być wpisywane także w szerszą, dopiero rozwijającą się ideę cyfrowej suwerenności Europy. Niesprawiedliwie niskie opodatkowanie technologicznych gigantów jako zagrożenie dla rozwoju gospodarczego UE przedstawiał na przykład raport *Conseil économique, social et environnemental* ciała doradczego francuskiego rządu z 2019 roku⁵¹. W tym samym roku Francja jako pierwszy kraj Wspólnoty przyjęła wzorowany na projekcie Komisji Europejskiej podatek od usług cyfrowych⁵². **Rzeczywistość bardzo szybko udowodniła, że prawo do regulowania, w tym opodatkowywania, międzynarodowych korporacji stanowi jeden z kluczowych aspektów cyfrowej suwerenności.** Działania Francji spotkały się bowiem z ostrym sprzeciwem Stanów Zjednoczonych, które stanęły w obronie wywodzących

się z kraju firm. Po wymianie gróźb celnych rząd Emmanuela Macrona zgodził się wstrzymać ściąganie opłaty na rok⁵³. Zarówno Francja, jak i inne kraje europejskie, które w międzyczasie wprowadziły cyfrowe podatki, wróciły do ich ściągania w 2021 roku⁵⁴, deklarując ich zawieszenie dopiero, gdy osiągnięte zostanie porozumienie w tej sprawie na forum OECD.

Próbę dołączenia do wąskiego grona krajów UE praktykujących cyfrową suwerenność w obszarze fiskalnym podjęto także w Polsce. W marcu 2020 roku Fundacja InStrat przedstawiła w tej sprawie obszerną ekspertyzę⁵⁵. Do animowania starań, by przyjąć między innymi tę regulację, zawiązała w kwietniu koalicję na rzecz Polskiej Karty Suwerenności Cyfrowej⁵⁶. Poza podatkiem od usług cyfrowych proponowała ona także między innymi wprowadzenie systemu oceny skutków algorytmów, który miałby badać ich wpływ na konkurencję i konsumentów, czy też inicjatywy służące ochronie praw pracowników platformowych⁵⁷. W listopadzie pomysł wprowadzenia w Polsce DST zmaterializował się w postaci złożonego przez Lewicę projektu ustawy o podatku od niektórych usług cyfrowych i Funduszu Technologii Cyfrowych. W uzasadnieniu wnioskodawcy pisali: „**[r]ozpoczęcie prac nad polskim podatkiem cyfrowym będzie świadczyć o gospodarczej i cyfrowej suwerenności naszego państwa, a zarazem będzie wyrazem solidarności z krajami europejskimi, które już rozpoczęły takie prace**”⁵⁸. Projekt przepadł w 2021 roku.

W chwili publikowania tego raportu w Polsce ponownie toczy się gorąca debata o podatku od usług cyfrowych. Kolejny raz jej inicjatorami są politycy związani z parlamentarną Lewicą oraz Fundacja InStrat, która przygotowała nową ekspertyzę w tym zakresie⁵⁹. Podobnie jak w 2020 r. wokół inicjatywy tworzy się oddolny ruch poparcia⁶⁰. Znowu też danina ta wpisywana jest w koncepcję cyfrowej suwerenności. Jak mówił w wywiadzie dla „Dziennika Gazety Prawnej” minister cyfryzacji Krzysztof Gawkowski: „[p]odatek cyfrowy pokaże (...) troskę o suwerenność technologiczną kraju i dowiedzie, że nie tylko o tym mówimy, ale i działamy”⁶¹.



2020: PANDEMICZNY KRYZYS BEZPIECZEŃSTWA GOSPODARCZEGO

Świadomość, że suwerenność w obszarze technologii ma fundamentalne znaczenie dla bezpieczeństwa gospodarczego UE, zaczęła kiełkować już w okresie poprzedniej kadencji Komisji Europejskiej, kierowanej przez Jean-Claude’a Junckera. Od 2017 roku realizowała między innymi inicjatywy partnerstw przemysłowych mających „łączyć szerokie grono partnerów z danej branży lub łańcucha wartości, w tym podmioty publiczne i prywatne oraz społeczeństwo obywatelskie”⁶². Zintensyfikowała też wsparcie dla wykorzystania mechanizmu *Important Projects of Common European Interest* (IPCEI)⁶³. Działania te miały na celu zarówno zwiększać odporność Europy, jak również ją integrować.

Jednym z haseł, które napędzały projekt, była „europejska suwerenność” – wiązane przede wszystkim z Macronem pojęcie, którego popularność wzrosła po kryzysie Brexitu⁶⁴. Przejęte przez Junckera, znalazło się w tytule jego orędzia o stanie Unii z 2018 roku. Deklarował w nim: „[g]eopolityka uczy nas, że przyszedł czas na europejską suwerenność”⁶⁵. W proponowanym przez niego i innych przywódców europejskich ujęciu oznaczała ona jednak przede wszystkim zacieśnianie współpracy w zakresie obronności oraz domykanie jednolitego rynku, niekoniecznie zaś ambicje w obszarze budowania własnych zdolności tworzenia produktów i usług związanych z nowymi technologiami. **Projekty IPCEI związane z mikroelektroniką⁶⁶ czy bateriami⁶⁷,**

jak również niemiecko-francuska inicjatywa Gaia-X dotycząca usług chmurowych wskazywały, że istnieje świadomość potrzeby uniezależniania się Europy od państw trzecich w tym obszarze. Nie był to jednak temat priorytetowy.

Jego ważność wzrosła w retoryce następczyni Junckera. Jeszcze zanim Ursula von der Leyen została wybrana przewodniczącą Komisji, w swoim manifest programowym deklarowała: „Europa już wyznacza standardy w telekomunikacji. Czas powtórzyć ten sukces i opracować wspólne standardy dla naszych sieci 5G. Być może jest już za późno, aby zreplikować hiperskalerów, ale nie jest za późno, aby osiągnąć suwerenność technologiczną w kluczowych obszarach technologicznych”⁶⁸. Kilka miesięcy później, prezentując program prac Komisji na 2020 rok, nowi komisarze precyzowali plany realizacji tych ambicji.

Czarny łabędź pandemii koronawirusa w 2020 roku zmusił Unię Europejską do przyspieszenia zabiegów służących podniesieniu odporności wspólnoty⁶⁹. Dotyczyło to szczególnie konieczności szybkiego zajęcia się słabościami łańcuchów dostaw w krytycznych obszarach gospodarki związanych z nowymi technologiami. By ocenić skalę problemu, Komisja zleciła badanie strategicznych zależności⁷⁰ służące aktualizacji nowej strategii przemysłowej⁷¹.

Jako najbardziej narażone ekosystemy, raport wyróżnił między innymi te związane z cyfrowymi produktami i usługami; obronnością, lotnictwem i kosmosem; elektroniką. Wskazał również konkretne produkty i usługi, wokół których stworzyły się wąskie gardła: między innymi półprzewodniki, przetwarzanie brzegowe (obliczenia wykonywane blisko źródła danych, zwykle w tym samym urządzeniu, które je generuje) i w chmurze, akumulatory litowo-jonowe. Zmapował wreszcie, od jakich krajów Unia Europejska jest uzależniona najsilniej w pozyskiwaniu produktów dla kluczowych ekosystemów. Na pierwszym miejscu znalazły się Chiny; pierwszą piątkę uzupełniały Wietnam, Brazylia, Korea i Singapur.

Czarny łabędź pandemii koronawirusa w 2020 roku zmusił Unię Europejską do przyspieszenia zabiegów służących podniesieniu odporności wspólnoty.

Alarmujący raport wspominał technologiczną suwerenność przelotnie, odwołując się do opublikowanego kilka miesięcy wcześniej planu działań Komisji w sprawie synergii między przemysłami cywilnym, obronnym i kosmicznym⁷². Ten dokument, który nie tylko w Polsce przeszedł bez echa, dobrze pokazał rozwijające się w obliczu pandemii defensywne rozumienie suwerenności technologicznej. Jak pisali jego autorzy: „[o]kreślenie, które technologie krytyczne wnoszą decydujący wkład w kluczowe zdolności, może pomóc w podjęciu decyzji: (i) które technologie są ważne z punktu widzenia suwerenności technologicznej (tj. w przypadku, gdy istnieje potrzeba zmniejszenia ryzyka zależności); (ii)

w których przypadkach połączone/skoordynowane wsparcie z różnych programów i instrumentów UE może sprostać takim wyzwaniom. **Aby wzmocnić swoją suwerenność technologiczną, UE musi utrzymać solidne kompetencje przemysłowe oraz, o ile to możliwe, dążyć do objęcia wiodącej roli w zakresie tych krytycznych technologii**”⁷³.

Od 2021 roku odwołania do techsuwerenności zaczęły być stałym elementem unijnych dokumentów programowych i legislacji. Pojawiały się między innymi w europejskim akcie ws. czipów⁷⁴, programie polityki „Droga ku cyfrowej dekadzie” do 2030 roku⁷⁵ czy rozporządzeniu w sprawie ustanowienia platformy na rzecz technologii strategicznych dla Europy (STEP)⁷⁶. Co istotne, **z biegiem czasu zaczęto poszerzać zakres celów, z którymi łączona jest technologiczna czy cyfrowa suwerenność. Dziś powszechnie przyjmuje się już, że nie dotyczy ona wyłącznie bezpieczeństwa gospodarczego, ale może służyć także innym celom związanym przede wszystkim z podnoszeniem dobrobytu Europejczyków.** Do tego, by Europa dostrzegła te szanse i zaczęła wyznaczać sobie coraz ambitniejsze cele, potrzebny był jednak niestety pandemiczny szok.



2022: PEŁNOSKALOWA INWAZJA ROSJI NA UKRAINĘ

Tocząca się od 2022 roku wojna – zarówno obronna narodu ukraińskiego, jak i hybrydowa, która dotyczy też Polski – to kolejny wstrząs, który zmusił Europę do przemyślenia, które technologie są krytyczne dla jej suwerenności. Kluczową część odpowiedzi na to pytanie stanowią technologie wojskowe⁷⁷: amunicyjne, pancerne czy artyleryjskie. Analiza tego aspektu techsuwerenności pozostaje jednak poza zakresem przedmiotowym niniejszego raportu. Poza wzrostem znaczenia tematyki przemysłu zbrojeniowego w UE, ważnym skutkiem wojny za wschodnią granicą był wzrost zainteresowania technologiami podwójnego zastosowania.

Zacieranie się granic między cywilnymi przemysłami technologicznymi – szczególnie w branżach kosmicznej, teleinformatycznej i lotniczej – a przemysłem obronnym to trend obserwowalny na świecie od dawna. Jednakże, jak zwracał uwagę raport Sauliego Niinistö *Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness*, w Europie ta współpraca nie funkcjonuje dobrze. Tymczasem „[s]ektor cywilny jest głównym motorem innowacji w dziedzinie zaawansowanych technologii, wyznaczając kierunki rozwoju kluczowych zdolności i zastosowań, które są następnie wykorzystywane w sektorze obronnym. Ten drugi musi być w stanie wykorzystać znacznie szybsze cykle innowacji cywilnych w zakresie technologii o potencjale podwójnego zastosowania, **aby utrzymać swoją konkurencyjność i zapewnić przewagę wojskową na polu walki. Dlatego też, aby nadal realizować potencjał innowacyjny, ważne jest inwestowanie w najnowocześniejsze technologie cywilne, które mogą później uzyskać zastosowania obronne**”⁷⁸. Choć raport Niinistö nie mówi wprost o techsuwerenności, to odwołuje się do niej pośrednio. Przypomina na przykład o wspomnianym już planie działań w zakresie synergii między przemysłem cywilnym, obronnym i kosmicznym, który z kolei wprost posługuje się tym terminem.

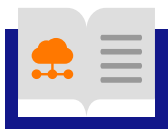
Wojna w Ukrainie pokazała światu, jakiego rodzaju krytyczne technologie podwójnego zastosowania są dziś kluczowe z perspektywy obronności. **Są to w pierwszej kolejności drony i systemy antydronowe⁷⁹, w drugiej zaś produkty i usługi branży kosmicznej, głównie systemy obserwacji Ziemi⁸⁰ i łączności satelitarnej.** W obu branżach – dronowej i kosmicznej – szeroko wykorzystywane są także systemy sztucznej inteligencji. Synergie między tymi obszarami otwierają pole do licznych współprac. Przykłady to partnerstwo fińsko-polskiej spółki ICEYE z polską firmą Satim dotyczące wykorzystania SI do identyfikacji obiektów na zobrazowaniach radarowych⁸¹ czy współpraca niemieckich startupów Helsing i ARX Robotics w zakresie systemów kontroli naziemnych pojazdów bezzałogowych⁸².

Ważną lekcją dla Europy płynącą z Ukrainy była niestety ta dotycząca spadku zaufania do wsparcia amerykańskiego rządu i przedsiębiorstw. W świadomości Europejczyków najsilniej zapisała się historia niejasnego udziału Elona Muska w zatrzymaniu ataku ukraińskich dronów na rosyjskie okręty w Sewastopolu⁸³. Mniej głośnym, choć także znaczącym epizodem wojny było zaprzestanie dostarczania Ukrainie obrazowań satelitarnych przez amerykańską spółkę Maxar Technologies w związku z czasowym zawieszeniem finansowego wsparcia Waszyngtonu dla Kijowa⁸⁴.

Towarzysząca inwazji na Ukrainę, a **trwająca do dziś hybrydowa wojna Moskwy z europejskimi sojusznikami Kijowa jest testem techsuwerenności rozumianej jako odporność na cyberzagrożenia**⁸⁵. Szczególnie przekonała się o tym Polska, gdzie powoli rozwija się świadomość, że „we wrogim kontekście każdy zasób i każda technologia mogą zostać wykorzystane jako broń, lub też w kreatywny sposób do obrony suwerenności”⁸⁶. Nie sposób też nie wspomnieć o atakach na fizyczną infrastrukturę stanowiącą fundament cyfrowej suwerenności Europy. To przede wszystkim liczne incydenty związane z kablami podmorskimi na dnie Bałtyku, a także groźne przypadki zagłuszania sygnału GPS. W warunkach zagrożenia związanego choćby z aktami sabotażu na znaczeniu rośnie potrzeba zabezpieczania nie tylko elektrowni czy wodociągów, ale też infrastruktury telekomunikacyjnej, centrów danych, superkomputerów, czy ośrodków produkcyjnych zaawansowanych technologii. Potrzeba dbania o bezpieczeństwo fizycznej infrastruktury służącej techsuwerenności istniała już wcześniej, choćby w związku z kryzysem klimatycznym. Bliskość frontu i bezwzględność działań Rosji w Europie dołożyły jednak nowe zagrożenia, szczególnie dla jej środkowo-wschodniego regionu.

Zagrożenia związane z wojną w Ukrainie odnoszą się więc do techsuwerenności w niemal każdym z wymienionych dotychczas kontekstów. Cyberataki zagrażają bezpieczeństwu danych Europejczyków, zaś obszar łańcucha dostaw jest celem 10,6 proc. ataków⁸⁷. Nieustannie wykrywane są zagrażające integralności UE kampanie dezinformacyjne prowadzone za pośrednictwem platform społecznościowych⁸⁸. Wojna tworzy też wyzwania dla łańcuchów dostaw: technologii militarnych i *dual-use*⁸⁹ czy też np. metali ziem rzadkich⁹⁰. By móc radzić sobie z tymi problemami, Europa potrzebuje technologicznej suwerenności.





2024: TRZY RAPORTY I PROGRAM NOWEJ KOMISJI EUROPEJSKIEJ

W roku wyborów europejskich uwagę osób interesujących się polityką europejską skupiona była nie tylko na wynikach głosowania, lecz także na trzech raportach zamówionych przez Komisję Europejską. Dokumenty sygnowane nazwiskami Maria Draghiego, Enrika Letty i Sauliego Niinistö miały istotnie wpłynąć na program nowej Komisji – niezależnie od tego, kto wejdzie do jej składu. Każdy z nich w mniejszym lub większym stopniu odnosił się do technologicznej suwerenności.

Jak zostało już wspomniane, najmniej bezpośrednio adresuje tę ideę raport Niinistö. To, że nie posługuje się pojęciem technologicznej ani cyfrowej suwerenności, nie znaczy jednak, że się do niej nie odnosi. Istotne z tej perspektywy wątki znaleźć można na przykład w części poświęconej rekomendacjom dla wzmocnienia odporności i przygotowania na kryzysy sektora prywatnego⁹¹. Niinistö pisze między innymi o wzmacnianiu cyberbezpieczeństwa infrastruktury energetycznej, większym zaangażowaniu biznesu w *derisking* czy o ochronie kabli podmorskich.

Raport Letty również nie zawiera wielu odniesień do pojęcia techsuwerenności. Znalazły się w nim jednak postulaty kojarzone z tymi dążeniami: dotyczące potrzeby inwestowania w infrastrukturę łącznościową oraz konsolidacji rynku telekomunikacyjnego w celu osiągnięcia korzyści z efektów skali. Gdy zaś Letta przywołuje samo pojęcie, rozumie je bardzo wąsko, łącząc je z bezpieczeństwem cyfrowym. Jak pisze: „u podstaw wspólnego interesu publicznego leżą dwa kluczowe elementy: cyberbezpieczeństwo i suwerenność cyfrowa”⁹². Jego propozycje dotyczą takich kwestii jak ograniczanie barier administracyjnych spowalniających rozwój sieci gigabitowych; usuwanie przeszkód utrudniających transgraniczną działalność w zakresie cyberbezpieczeństwa; ujednolicenie polityki dotyczącej przyznawania i wykorzystywania pasm częstotliwości.

Najwięcej uwagi techsuwerenności poświęca raport Draghiego. Łączy poparcie dla idei ze sceptycyzmem co do tego, w jakim stopniu Europa jest w stanie zbudować konkurencję wobec Stanów Zjednoczonych w obszarach technologicznych. Nie zmienia to faktu, że zamykanie „luki innowacyjności” stanowi główny postulat raportu⁹³.

Podobnie jak von der Leyen w 2019 roku, tak i Draghi pięć lat później stwierdza, że Europa „przegrała” rynek chmurowy. W tej sytuacji kluczowe jest dla niego, „aby przedsiębiorstwa z UE utrzymały pozycję w obszarach wymagających suwerenności technologicznej, takich jak bezpieczeństwo i szyfrowanie (rozwiązania typu »suwerenna chmura«)”⁹⁴. Chodzi o model, w którym dostawcy usług *Infrastructure as a Service* z UE współpracują z amerykańskimi hiperskalarami specjalizującymi się w obliczeniach rozproszonych, zachowując kontrolę nad wrażliwymi elementami ekosystemu. Draghi przyznaje, że nie jest to rozwiązanie w pełni suwerenne, ale stanowi jego zdaniem najlepszą dostępną alternatywę dla europejskich hiperskalerów, których brak na rynku⁹⁵. Sugeruje wreszcie dwutorowe podejście do regulacji rynku chmurowego. Tam, gdzie „suwerenność” usług jest niezbędna, Europa powinna wprowadzić wspólne standardy zamówień publicznych. W innych obszarach rozwijać z kolei w partnerstwie z USA „cyfrowy rynek transatlantycki” z niskimi barierami wejścia⁹⁶.

Oprócz chmury, Draghi wyróżnia także kwestie suwerenności w obszarach sztucznej inteligencji i informatyki kwantowej. Jego zdaniem Europa ma wciąż szanse, by dołączyć w nich do grona liderów. Musi jednak zwiększyć inwestycje publiczne w zasoby obliczeniowe, przede wszystkim centra superkomputerowe w ramach programu Euro-HPC, a także doprowadzić do wzrostu inwestycji prywatnych w technologie kwantowe⁹⁷. Do pojęcia suwerenności technologicznej Draghi odwołuje się również między innymi przy omawianiu wsparcia dla branż kosmicznej oraz półprzewodnikowej.

Postulaty Draghiego, choć krytykowane przez część ekspertów (na przykład za zbyt ni nacisk na inwestycje infrastrukturalne⁹⁸), stały się de facto doktryną drugiej Komisji Ursuli von der Leyen. Jak pisała w programie na lata 2024-2029: „[z]intensyfikujemy nasze inwestycje w kolejną falę przełomowych technologii, w szczególności w superkomputery, półprzewodniki, internet rzeczy, genomikę, informatykę kwantową, technologie kosmiczne i inne”⁹⁹. Zobowiązała się też do zwiększenia wysiłków na rzecz poprawy innowacyjności Europy w obszarze SI, czemu służyć ma przedstawiony w kwietniu *Plan działania na rzecz kontynentu sztucznej inteligencji*¹⁰⁰. Choć hasło suwerenności technologicznej tym razem nie pojawiło się w manifestie kandydatki na przewodniczącą KE, to trafiło do tytułu nowej wiceprzewodniczącej Komisji, Henny Virkkunen. U progu nowej kadencji Bruksela starała się wysłać krajom członkowskim jasny sygnał, że wsparcie przemysłu technologicznego – od centrów badawczo-rozwojowych i startupów po narodowych czempionów – w służbie konkurencyjności gospodarczej UE będzie w centrum jej agendy.



2025: KRYZYS RELACJI TRANSATLANTYCKICH PO ZWYCIĘSTWIE DONALDA TRUMPA

W ciągu dekady debat o techsuwerenności w UE poszerzyło się grono zaangażowanych w nią środowisk: od akademików i thinktankerów do przywódców państw. Zwiększyła się liczba poruszanych w niej wątków: od ochrony prywatności Europejczyków po politykę konkurencji. W konsekwencji rosta ważność tematu. Techsuwerenność z zagadnienia istotnego, ale nie centralnego, awansowała do rangi, używając określenia Draghiego, „wyzwania egzystencjalnego”¹⁰¹.

Tak przynajmniej w połowie 2024 roku sytuacja kształtowała się na poziomie retoryki. W praktyce dążenia do suwerenności technologicznej napotykały trudności. Europa wydawała się pogodzona ze status quo na rynku chmurowym, sprowadzając siebie do roli partnera amerykańskich hiper-skalerów, choć oznaczał on jej uzależnienie od firm z państw trzecich. Egzekwowanie cyfrowych konstytucji postępowało powoli, mimo apeli biznesu¹⁰² i organizacji pozarządowych¹⁰³, między innymi z powodu opieszałości państw członkowskich w implementowaniu przepisów¹⁰⁴. Rosło ryzyko, że Europa nie osiągnie celów cyfrowych, które wyznaczyła sobie do 2030 roku¹⁰⁵. Obawy budził też kierunek inwestycji UE, skupiony na wąskiej kategorii „technologii dysruptywnych”¹⁰⁶, traktując raczej po macoszemu tworzenie cyfrowych dóbr publicznych¹⁰⁷ mimo dowodów skuteczności takich inicjatyw jak *Next Generation Internet*¹⁰⁸.

U progu kadencji nowej Komisji Europejskiej rozpoczęły się zabiegi, by wpłynąć na to, jak rozumiana w jej trakcie będzie cyfrowa suwerenność. Pod koniec września 2024 r., gdy wciąż nie wiadomo było, kto zwycięży w wyborach prezydenckich w USA, w Brukseli odbyła się konferencja *Toward European Digital Independence*. Współorganizowana przez wszystkie największe partie w Parlamencie Europejskim, promowała świeżą wówczas ideę EuroStacka: budowy europejskiego stosu technologicznego, publicznej cyfrowej infrastruktury o szerokim spektrum zastosowań¹⁰⁹.

Nie brakowało jednak także głosów, że rozumienie techsuwerenności powinno ewoluować w innym kierunku. Na łamach portalu Politico Mark Scott i Konstantinos Komaitis, eksperci z Atlantic Council, przekonywali, że „suwerenność technologiczna» to coś więcej niż tylko tworzenie zasad cyfrowych, które chronią przed szkodami. Może obejmować wspieranie przedsiębiorczości, promowanie otwartych rynków i finansowanie najlepszych pomysłów na świecie”¹¹⁰.

Ultimatum administracji
Trumpa zakłada, że
UE zrezygnuje
z suwerenności
w obszarze regulacji
i sprzymierzy się
z USA albo znajdzie się
w obozie przegranych
w wyścigu
technologicznym.

Wydarzenia za oceanem narzuciły tym dyskusjom nowe ramy. Jasne stało się przede wszystkim, że trudno będzie kontynuować odbudowę partnerskich relacji z USA. Za prezydentury Joe Bidena ważną rolę w tym procesie odgrywała powołana w 2021 roku Rada ds. Handlu i Technologii. Po 6 listopada 2024 roku jej przyszłość stanęła pod znakiem zapytania¹¹¹. **Niektórzy analitycy spraw międzynarodowych sugerowali wręcz w tej sytuacji zarzucenie idei cyfrowej suwerenności na rzecz cyfrowej solidarności: transatlantyckiego sojuszu antychińskiego, w którym Europa godzi się na rolę biorcy amerykańskich technologii**¹¹². Inni wskazywali z kolei, że zwycięstwo Trumpa wspieranego w dużej mierze przez krajową branżę tech powinno być ostrzegą dla UE, aby w suwerennościowych dążeniach nie powielić patologii Doliny Krzemowej¹¹³.

Póki jednak republikanie nie objęli rządów w Waszyngtonie, rozważania te stanowiły mniej lub bardziej zakorzenione w faktach spekulacje. Europa trwała w oczekiwaniu, czy początek kadencji Trumpa potwierdzi jej obawy, czy da powody do optymizmu. **Zgodnie z maksymą o tygodniach, w których dzieją się dekady, kilkanaście dni w lutym dało odpowiedzi na wiele pytań co do przyszłości transatlantyckiego partnerstwa technologicznego.** 11 lutego podczas szczytu „AI Action” w Paryżu wiceprezydent USA J. D. Vance wykonał otwierającą salwę w toczącym się do dziś transatlantyckim sporze o cyfrowe regulacje¹¹⁴. Atakował DSA i RODO jako akty wrogie amerykańskim firmom technologicznym. Podkreślał też skalę planowanych w USA inwestycji w sztuczną inteligencję, które do 2028 roku mają rzekomo osiągnąć poziom 800 miliardów dolarów. Wydzźwięk tej przemowy był jasny: albo UE sprzymierzy się z USA na narzuconych sobie zasadach, rezygnując z suwerenności w obszarze regulacji, albo znajdzie się w obozie przegranych w wyścigu technologicznym. Podobnie konfrontacyjny ton Vance obrał kilka dni później podczas konferencji bezpieczeństwa w Monachium¹¹⁵. 21 lutego nowe, agresywne podejście do europejskich cyfrowych konstytucji zostało ostatecznie skodyfikowane w prezydenckim memorandum¹¹⁶.

Na reakcję Europy nie trzeba było długo czekać. Jeszcze w trakcie paryskiej konferencji Ursula von der Leyen zapowiedziała inicjatywę *Invest AI*, w ramach której powstanie fundusz wsparcia sztucznej inteligencji o wartości 20 miliardów euro¹¹⁷. Równolegle ponad 60 podmiotów sektora prywatnego ogłosiło inicjatywę EU AI Champions, deklarując, że w ciągu 5 lat alokują w UE 150 miliardów euro, o ile Europa obierze bardziej prokonkurencyjny kurs względem nowych technologii. W Monachium komisarka Virkkunen przekonywała, że regulacje sieci są jedynie przedłużeniem podstawowych praw chroniących Europejczyków *offline*. Komisarz ds. handlu Maroš Šefčovič podkreślał zaś 19 lutego w Waszyngtonie, że UE w negocjacjach celnych będzie bronić DSA i DMA.

13 lutego ukazał się długo wyczekiwany raport *EuroStack – A European Alternative for Digital Sovereignty*¹¹⁸. Komentując tę premierę, Martin Hullin i Teresa Staiger z Bertelsmann Stiftung, która go zamówiła, wskazywali dokument jako adekwatną odpowiedź na nową politykę USA. „Podczas szczytu AI Action Summit wiceprezydent J. D. Vance skrytykował europejskie podejście regulacyjne, sugerując, że nadmierna regulacja może hamować postęp technologiczny amerykańskich platform technologicznych” – pisali. – „Ta krytyka i publiczne poparcie branży dla administracji Trumpa podkreślają pilną potrzebę opracowania przez Europę własnych solidnych ram cyfrowych w celu zachowania autonomii technologicznej”¹¹⁹.

Podczas dwóch intensywnych lutowych tygodni wiele w temacie techsuwerenności wydarzyło się także w Polsce. 10 lutego premier Donald Tusk zapowiedział, że Polska w ramach wsparcia rozwoju nowych technologii poszerzy współpracę z firmami takimi jak Google, Microsoft, Amazon i IBM. Ogłosił, że spotka się z przedstawicielami dwóch pierwszych z wymienionych spółek. Szczególnie głośnym echem odbiła się konferencja Tuska z Sundarem Pichaiem (dyrektorem generalnym Google). Omawiając ogłoszone w jej trakcie skromne zapowiedzi inwestycji i niejasne deklaracje co do udziału Google w transformacji energetycznej i reformie systemu opieki zdrowia w Polsce¹²⁰ wielu komentatorów wskazywało, na potrzebę mocniejszego uwzględnienia **zachodzącej w Unii Europejskiej korekty kursu względem zacieśniania współpracy z amerykańskimi firmami, z czym wiąże się też wzrost poparcia dla cyfrowego patriotyzmu gospodarczego**¹²¹.

Kolejne miesiące przynosiły liczne przykłady tego trendu. 27 marca przedstawiciele państw z grupy D9+ (do której należy też Polska), tradycyjnie postrzeganych jako przeciwnicy protekcjonizmu, podpisali Deklarację Amsterdamską wzywającą Komisję Europejską do „zwiększenia konkurencyjności cyfrowej UE i jej niezależności technologicznej w otwarty sposób”¹²². Kilkanaście dni później przedstawiciele rządów Francji i Niemiec oficjalnie poparli założenia inicjatywy EuroStack¹²³. W lipcu zaś europarlamentarna komisja przemysłu, badań naukowych i energii (ITRE) przyjęła wspólny raport w sprawie europejskiej suwerenności technologicznej i infrastruktury cyfrowej¹²⁴.

W dokumencie ITRE wzywa Unię Europejską do utworzenia w budżecie na lata 2028-2034 osobnego funduszu na rozwój publicznej infrastruktury cyfrowej. **Zakorzenianie się pojęcia publicznej infrastruktury cyfrowej w europejskim dyskursie o techsuwerenności to jeden z najważniejszych trendów ostatnich miesięcy**¹²⁵. Opisywany wcześniej dryf w polityce przemysłowej Europy – od kreowania rynku do kierowania rynkiem – uzupełni być może kolejny zwrot: ku kreowaniu cyfrowych dóbr wspólnych. Ich przykłady to otwarte: oprogramowanie, systemy sztucznej inteligencji, dane czy repozytoria treści¹²⁶. Jako fundament publicznej infrastruktury cyfrowej mogą być źródłem wielu korzyści społecznych – poprawy cyfrowych kompetencji czy cyfryzacji sektora publicznego. Ten potencjał zaczynają dostrzegać niektóre europejskie rządy. W lipcu Niemcy, Francja, Włochy i Holandia ogłosiły zamiary powołania inicjatywy *European Digital Infrastructure Consortium (EDIC) for Digital Commons*, by przy wsparciu finansowym z UE rozwijać między innymi oprogramowanie biurowe dla administracji¹²⁷.

O ile budowa cyfrowej infrastruktury publicznej to pieśń przyszłości, o tyle wsparcie tworzenia infrastruktury cyfrowej w obszarach uznawanych przez Brukselę i państwa członkowskie za krytyczne staje się nową normalnością. Ilustrują to przykłady takie jak tworzenie suwerennych mocy obliczeniowych dla sztucznej inteligencji poprzez program fabryk i gigafabryk, budowa własnego systemu łączności satelitarnej IRIS2¹²⁸ czy europejska strategia kwantowa¹²⁹. Polska również w nich uczestniczy.

To świadectwo tego, jak mocno przez ostatnią dekadę przesunęło się okno Overtona. Dziś, gdy nikogo nie dziwią miliardowe inwestycje w najnowsze technologie (nawet jeśli bywają krytykowane¹³⁰), na obrzeżach dyskursu rodzą się bardziej radykalne idee, jak cyfrowy *decoupling* od USA¹³¹.

Idea techsuwerenności ma dziś szerokie społeczne poparcie. Według sierpniowego badania FGS Global za ważną uważa ją aż 91 proc. Niemców, 89 proc. Francuzów, 84 proc. Włochów¹³². Czas pokaże, w jakim kierunku rozwinie się ta idea. Bo to, że będzie ewoluować – tak w warstwie retorycznej, jak i w praktyce działań państwa, biznesu, społeczeństwa obywatelskiego – jest raczej pewne.

1.4. Czemu służy techsuwerenność

Patrząc na historię idei suwerenności technologicznej w Europie, można wyróżnić szereg deklaracji na temat celów, które ma ona realizować. Ta niejednoznaczność to jej funkcjonalność, a nie wada. Dzięki niej podmioty o różnych poglądach społecznych, gospodarczych, politycznych są w stanie zawiązywać sojusze pod wspólnym hasłem. Mówiąc bardziej konkretnie, teoretycy europejskiego dyskursu polityczno-gospodarczego zauważają, że „[s]uwerenność technologiczna łączy podmioty mające cele gospodarcze lub związane z bezpieczeństwem z tymi o celach »aspiracyjnych«”¹³³. O słuszności tej obserwacji świadczy na przykład kształt koalicji EuroStack¹³⁴. Tworzą ją przedstawiciele dużego, małego i średniego biznesu, różnych frakcji w Parlamencie Europejskim, akademicy i niezależni aktywiści działający na rzecz poprawy gospodarki cyfrowej.

Zadania, które różne środowiska starają się realizować poprzez działania związane z zabiegami o techsuwerenność, można pogrupować w trzy oddzielne, ale niewykluczające się wzajemnie kategorie¹³⁵. Są to: **wykonywanie podstawowych funkcji państwa, budowa konkurencyjnej gospodarki oraz transformacja systemowa**. By lepiej zilustrować tę koncepcję, poniżej wyszczególnione i opisane zostały po dwa przykłady konkretnych celów w ramach każdej kategorii.





WYKONYWANIE FUNKCJI PAŃSTWA

Ochrona europejskich praw i wartości

Prawodawstwo to jedna z podstawowych funkcji władzy państwa i uprawnionych instytucji ponadnarodowych. Składa się na nią nie tylko stanowienie, ale i egzekwowanie prawa. Obecna sytuacja, w której Unia Europejska uzależniona jest od państw trzecich, ogranicza realizowanie tej funkcji. Przykłady ilustrujące ten problem to choćby amerykańskie groźby sankcji za nakładanie cyfrowych podatków; nacisk na Europę, by nie egzekwowała wobec firm z USA przepisów DSA i DMA. Suwerenność technologiczna może dać Europie wolność w aspekcie negatywnym, to jest wolność od presji, by pod groźbą odcięcia od krytycznych technologii czy powszechnie używanych usług zarzuciła stanowienie i egzekwowanie konkretnych praw¹³⁶. Techsuwerenność może być także źródłem wolności pozytywnej. Bez niej trudno chociażby zapewniać obywatelom prawo do prywatności cyfrowych danych. W technologicznie suwerennej UE łatwiej byłoby realizować wolności spisane w Europejskiej deklaracji praw i zasad cyfrowych w cyfrowej dekadzie, jak na przykład prawo dostępu online do kluczowych usług publicznych¹³⁷. Nie posiadając własnej infrastruktury cyfrowej, UE nie jest w stanie gwarantować tego swoim obywatelom.

Zapewnianie bezpieczeństwa zewnętrznego

Państwo – samodzielnie i poprzez współpracę narodową – ma obowiązek zapewniać obywatelom bezpieczeństwo. Chodzi tu zarówno o bezpieczeństwo militarne, jak i na przykład ochronę przed skutkami katastrof naturalnych. By realizować ten cel, zobligowane do tego podmioty muszą posiadać odpowiednie środki technologiczne. Techsuwerenność ma więc gwarantować na przykład nieuzależniony od prywatnych firm z państw trzecich dostęp do bezpiecznej łączności i zdolności obserwacji Ziemi, czy też do pochodzących z zaufanych źródeł narzędzi (oprogramowania, sprzętu) ochrony krytycznej infrastruktury. W dążeniach do otwartej strategicznej autonomii chodzi nie tylko o zaspokajanie już zdiagnozowanych potrzeb, ale o antycypowanie przyszłych wyzwań. Lokalne inwestycje w badania i rozwój czy bazę produkcyjną sektorów cywilnych oraz sektora obronnego mają sprawić, że Europa będzie zdolna reagować na przyszłe kryzysy, jak ataki z użyciem nowych rodzajów broni czy pandemie nieznanych dotychczas chorób.



BUDOWA KONKURENCYJNEJ GOSPODARKI

Tworzenie warunków do rozwoju biznesu

„Eliminowanie luki innowacyjnej” to jeden z trzech filarów kompasu konkurencyjności dla UE¹³⁸. Cel ten jest nierozdzielnie związany z dążeniami do technologicznej suwerenności. Polityki takie jak tworzenie przyjaźniejszego otoczenia regulacyjnego i inwestycyjnego dla start-upów i scale-upów¹³⁹ czy wsparcie finansowe dla branży SI poprzez program fabryk i gigafabryk to przykłady działań, które zwiększają niezależność UE, tworząc jednocześnie warunki do rozwoju przedsiębiorstw. Poza wspieraniem innowacyjności Komisja Europejska chce też poprawić konkurencyjność poprzez „[z]mniejszenie nadmiernych zależności i zwiększenie bezpieczeństwa”. Związane z tymi ambicjami działania to na przykład planowany na przyszły rok przegląd dyrektywy w sprawie zamówień publicznych. Wpisuje się on w dążenia do suwerenności technologicznej

poprzez przyjęcie podejścia *Buy European*. Promowanie techsuwerenności i wspieranie europejskiego biznesu to dwie strony tej samej monety.

Wyrównywanie pola gry

Mając zdolność egzekwowania cyfrowych praw, technologicznie suwerenna Europa może lepiej zadbać o interesy lokalnych przedsiębiorstw, adresując na przykład poprzez DMA nieuczciwe praktyki konkurentów, niezależnie od kraju ich pochodzenia. Polityka wyrównywania pola gry dotyczy także rynku wewnętrznego Unii Europejskiej. Jako że techsuwerenność jest projektem wymagającym ścisłej kooperacji na poziomie ponadnarodowym, wiąże się z harmonizacją prawa i wprowadzaniem wspólnych standardów (czego przykładem są choćby pieczęcie suwerenności w ramach platformy STEP). Dzięki temu dążenie do suwerenności technologicznej Unii Europejskiej staje się narzędziem domykania jednolitego rynku.



TRANSFORMACJA SYSTEMOWA

Podwójna transformacja (zielona i cyfrowa)

Związek między techsuwerennością a cyfryzacją sektorów publicznego i prywatnego wydaje się intuicyjnie zrozumiały. Wsparcie dla lokalnego wytwarzania i wykorzystania technologii cyfrowych w efekcie tworzy bardziej zróżnicowany rynek produktów i usług. Podmioty wchodzące w transformację cyfrową mają większy wybór partnerów dla procesu, mogą łatwiej uniknąć pułapki uzależnienia od dostawcy (*vendor lock-in*) dzięki wsparciu dla interoperacyjności, wreszcie korzystają na większej konkurencji cenowej. Co więcej, technologiczna suwerenność rozumiana jako rozwój cyfrowych dóbr wspólnych może znacznie obniżyć koszt cyfryzacji, na przykład dzięki otwartemu oprogramowaniu i ekosystemowi wsparcia podobnych rozwiązań. Jak zauważają Zuzanna Warso i Jan Krewer: „[c]yfrowe dobra wspólne zdobywają uwagę polityków ze względu na potencjał zaspokajania zróżnicowanych potrzeb społecznych związanych z infrastrukturą cyfrową, takich jak (...) bardziej konkurencyjne środowisko cyfrowe, które poprawiłoby dostępność i jakość usług cyfrowych”¹⁴⁰. Praktycznym sposobem, w jaki można realizować ideę wsparcia cyfrowej transformacji administracji dzięki publicznej infrastrukturze cyfrowej, jest wspomnianą już inicjatywa *EDIC for Digital Commons*. Jeśli zaś chodzi o korzyści dla zielonej transformacji, to wiążą się one przede wszystkim z większą konkurencyjnością gospodarki. Likwidując lukę innowacyjności, Europa tworzy szansę na to, że będą powstawać rozwiązania wspierające dekarbonizację gospodarki. Podejmując działania na rzecz strategicznej autonomii, zyskuje z kolei większą kontrolę nad łańcuchami dostaw, co może pozwolić na ich „zazielenienie”.

Sprawiedliwa transformacja

W kontekście bliźniaczej transformacji trwają zabiegi, by była nie tylko zielona i cyfrowa, ale przede wszystkim sprawiedliwa. Jak zwraca uwagę Cecilia Rikap, „[s]trategiczny rozwój niektórych zastosowań technologii cyfrowych mógłby przyczynić się do skoordynowanej sprawiedliwej transformacji”¹⁴¹. Dążenia do techsuwerenności to ambitny projekt wymagający zacieśniania europejskiej integracji i dogłębnej refleksji nad rolą cyfryzacji w gospodarce i społeczeństwie. W tym sensie może być okazją, by zająć się kosztami społecznymi technologii, ale i ich potencjałem dla podnoszenia poziomu zaufania społecznego czy zmniejszania nierówności edukacyjnych.



Część 2. Praktyka

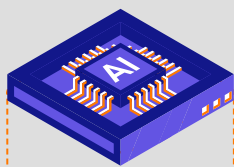
2.1. Stos technologiczny po polsku

Wspominany kilkakrotnie w niniejszym dokumencie EuroStack oznacza europejski stos technologiczny: pogrupowany w kategorie i ułożony warstwowo zbiór technologii tworzących współczesną gospodarkę cyfrową, od źródeł energii po pojedyncze aplikacje. Przedstawiony w głośnym raporcie z lutego 2025 roku model stosu stanowi „ramę koncepcyjną, gdzie każda warstwa opiera się na możliwościach warstwy poniżej niej, jednocześnie dynamicznie współdziałając z pozostałymi”¹⁴². **Rama ta ma zastosowanie praktyczne. Wizualizując efemeryczne pojęcie „infrastruktury” jako obszary, które nakładają się na siebie kolejnymi warstwami, pozwala łatwiej zrozumieć zależności i potrzeby związane z rozwojem całego ekosystemu.**

Koncepcja EuroStacku stoi w opozycji do strategii, które skupiają się na miejscowym wsparciu krytycznych punktów technologicznych w łańcuchach wartości. Zamiast decydować, czy istotniejsze z perspektywy suwerenności są superkomputery dla branży sztucznej inteligencji, kable podmorskie, czy aplikacje biurowe, proponuje podejście holistyczne.

Raport prezentujący koncepcję EuroStacka wylicza następujące warstwy stosu w kolejności od najwyższej¹⁴³ (👁️ patrz strona obok).

Stos technologiczny można podzielić na warstwy także na inne sposoby¹⁴⁴, jednak operacjonalizacja zaproponowana przez autorów raportu EuroStack jest jedną z najpopularniejszych. W ramach ćwiczenia analitycznego na potrzeby niniejszej publikacji przygotowana została **mapa polskich podmiotów mogących uczestniczyć w tworzeniu europejskiego stosu**. Podobną listę podmiotów europejskich znaleźć można w raporcie EuroStack¹⁴⁵.



1

Dane i sztuczna inteligencja (np. repozytoria danych, modele SI)

- » CampusAI (Warszawa)
- » DataWalk (Wrocław)
- » Fundacja SpeakLeash (Wrocław)
- » HIVE AI (Warszawa)
- » PIAST-AI (Poznań)



2

Internet rzeczy i urządzenia (np. systemy operacyjne, aplikacje)

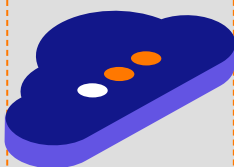
- » AIUT (Gliwice)
- » Fibar Group (Wysogotowo)
- » Łukasiewicz Instytut Tele- i Radiotechniczny (Warszawa)
- » Manta (Warszawa)
- » Maxcom (Tychy)
- » Wilk Elektronik (Łaziska Górne)



3

Platformy, oprogramowanie i algorytmy (np. smartfony, laptopy, czujniki)

- » Asseco (Rzeszów)
- » Polski Standard Płatności (Warszawa)
- » Comp (Warszawa)
- » Sygnity (Wrocław)
- » Symfonia (Warszawa)
- » Transition Technologies (Warszawa)



4

Infrastruktura chmurowa (np. centra danych, superkomputery)

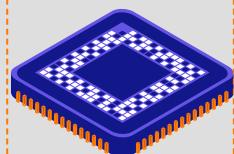
- » Asseco Cloud (Rzeszów)
- » Beyond Solutions (Poznań)
- » CloudFerro (Warszawa)
- » Cyfronet (Kraków)
- » OVH (Wrocław)



5

Sieci (np. wieże telekomunikacyjne, sieci światłowodowe, kable podmorskie)

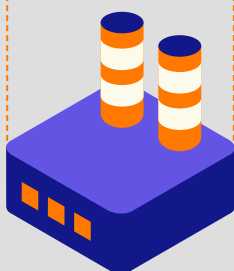
- » Exatel (Warszawa)
- » Fibrain (Głogów Małopolski)
- » IS-Wireless (Piaseczno)
- » Orange Polska (Warszawa)
- » P4 (Warszawa)
- » Polkomtel (Warszawa)
- » T-Mobile Polska (Warszawa)



6

Czipy (np. procesory graficzne i GPU, pamięć)

- » DCD-SEMI (Bytom)
- » Łukasiewicz – Instytut Mikroelektroniki i Fotoniki (Warszawa)
- » QNA Technology (Wrocław)
- » VIGO Photonics (Ożarów Mazowiecki)
- » XTPL (Wrocław)



7

Zasoby (np. metale ziem rzadkich, energia, kapitał ludzki)

Metodologia doboru podmiotów opierała się na czterech zasadach:

- » Ich struktura kapitałowa daje bezpośrednią kontrolę **podmiotom z Europy**.
- » Mają **główną siedzibę w Polsce**.
- » Posiadają **międzynarodowe doświadczenie**, które umożliwia im angażowanie się we współpracę przy budowie europejskiego ekosystemu.
- » Mają **dojrzałość rynkową**: choć na liście znajdują się start-upy i scale-upy, a nie tylko spółki giełdowe, to są to podmioty obecne dłuższy czas na rynku.

- | | | |
|--------------------------------|--------------------------------|---|
| 1 Dane i sztuczna inteligencja | 2 Internet rzeczy i urządzenia | 3 Platformy, oprogramowanie i algorytmy |
| 4 Infrastruktura chmurowa | 5 Sieci | 6 Czipy |



2.2. Finansowanie techsuwerenności

EuroStack stanowi przykład odpowiedzi na pytanie, na co w praktyce powinny być przeznaczane środki mobilizowane do realizacji idei techsuwerenności. Pozostaje jednak kwestia tego, skąd te środki czerpać. W debacie publicznej najczęściej wymieniane są następujące źródła.

Zamówienia publiczne

Planowany na przyszły rok przegląd dyrektywy o zamówieniach publicznych jest uważany za szansę, by wprowadzić ogólnounijne zasady wspierające lokalną branżę technologiczną. Klauzula *Buy European* miałyby zobowiązywać podmioty publiczne, by priorytetyzowały dostawców spełniających określone kryteria „europejskości”. Europa rozumiana jest tutaj nie jako Unia Europejska, ale kraje członkowskie Europejskiego Stowarzyszenia Wolnego Handlu (EFTA). Wśród kryteriów wskazuje się przede wszystkim następujące trzy¹⁴⁶:

- » Główna siedziba w Europie;
- » Większość działalności badawczo-rozwojowej w Europie;
- » Większościowa kontrola nad firmą sprawowana przez europejskie podmioty.

Inne propozycje dotyczą na przykład wykluczania technologii nieefektywnych energetycznie¹⁴⁷. Niektórzy eksperci wskazują wreszcie, że odpowiednio sformułowane zamówienia publiczne mogą już dziś faworyzować europejskie podmioty, nie naruszając prawa unijnego ani międzynarodowych porozumień¹⁴⁸.

Rynek kapitałowy

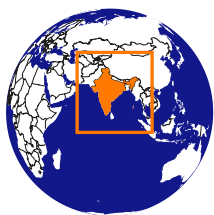
Jak wskazywał w swoim raporcie Mario Draghi: „[g]łówną przyczyną mniej efektywnego pośrednictwa finansowego w Europie jest fragmentacja rynków kapitałowych i niższy poziom przepływów oszczędności na rynki kapitałowe”¹⁴⁹. Podmioty rozporządzające kapitałem prywatnym – fundusze *venture capital* czy emerytalne¹⁵⁰ – stanowią poza Europą główne źródło finansowania inwestycji w technologie cyfrowe. Jak wskazywała KE w raporcie o stanie cyfrowej dekady, UE odpowiada jedynie za 5 proc. globalnego kapitału VC na innowacje, podczas gdy na Stany Zjednoczone przypada 52 proc. udziałów, a na Chiny 40 proc. Z kolei europejskie start-upy SI pozyskały w 2024 roku ponad sześć razy mniej finansowania z kapitału VC niż start-upy w Stanach Zjednoczonych¹⁵¹. Idąc za sugestiami Draghiego, Komisja Europejska przedstawiła w marcu plany utworzenia unii oszczędności i inwestycji¹⁵². Warto przy tym podkreślić, że amerykański model prywatnego finansowania technologii przez VC wymaga co najmniej przemysłu. Promowana w nim wizja błyskawicznego skalowania przedsiębiorstw nierzadko stoi w sprzeczności z ochroną praw pracowniczych czy zrównoważonym rozwojem¹⁵³. Realizując wartościowy projekt uwalniania prywatnych środków, niezbędnych dla projektów podnoszących techsuwerenność, Europa powinna odrobić lekcje oferowane przez analityków badających rynek kapitałowy w USA.

Fundusze unijne

Autorzy raportu EuroStack zaproponowali utworzenie funduszu o początkowej wartości 10 miliardów euro, którego wartość wzrosłaby 30-krotnie w ciągu dekady. Środki miałyby pochodzić od państw członkowskich, Europejskiego Banku Inwestycyjnego, inwestorów instytucjonalnych czy prywatnego kapitału¹⁵⁴. Z kolei raport komisji ITRE sugeruje osobną kopertę na publiczną infrastrukturę cyfrową w wieloletnich ramach finansowania¹⁵⁵. Pieniądze na cyfrową suwerenność można znaleźć w wielu obszarach europejskiego budżetu na lata 2028-2034. Przykładowo regulacja ustanawiająca nowy Fundusz Konkurencyjności¹⁵⁶ o wartości 410 miliardów euro zawiera odwołania do cyfrowej suwerenności i publicznej infrastruktury cyfrowej. Analiza NGO Open Future wskazuje również na inne środki budżetowe dla inicjatyw związanych z techsuwerennością (suwerenną chmurę, narzędzia do rozwoju cyfrowej demokracji), na przykład programy AgoraEU i InvestEU¹⁵⁷. Szansą na alokowanie przeznaczonych na techsuwerenność środków są wreszcie projekty typu *moonshot* (długoterminowe, o fundamentalnym znaczeniu dla Europy) w ramach programu Horyzont Europa. Rozwijana przez ekonomistkę Mariannę Mazzucato koncepcja polityki przemysłowej opartej na misjach¹⁵⁸, z którą powiązane są moonshoty, od dawna wskazywana jest jako inspiracja dla szeroko zakrojonych projektów uniezależniania infrastruktury technologicznej¹⁵⁹.

2.3. Techsuwerenność: lekcje ze świata

Niniejszy raport skupia się na dążeniach do technologicznej suwerenności w Europie, przede wszystkim na poziomie Unii Europejskiej. Ambicje w tym obszarze ma jednak dużo więcej graczy na globalnej arenie. Oczywistymi przykładami są Stany Zjednoczone i Chiny. Suwerennościowy zwrot Europy był w dużej mierze reakcją na ich dążenia, by dzielić i rządzić w globalnej gospodarce cyfrowej i innych sektorach technologicznych. Próbując z nimi konkurować, UE stara się jednocześnie inspirować niektórymi aspektami ich polityk przemysłowych. Źródła dobrych praktyk znaleźć można jednak także w innych częściach świata. Na zakończenie raportu prezentujemy kilka przykładów krajów, których dążenia do techsuwerenności są warte uwagi, ze wskazaniem kluczowych obszarów strategicznego namysłu.



INDIE

Od 2009 roku w Indiach rozwijany jest projekt publicznej infrastruktury cyfrowej znany powszechnie jako IndiaStack¹⁶⁰. Opiera się na „cyfrowym trójnogu”: elektronicznej tożsamości dla każdego mieszkańca (Aadhaar); interfejsie do cyfrowych płatności (*Unified Payments Interface*, UPI); architekturze zarządzania danymi (*Data Empowerment and Protection Architecture*, DEPA)¹⁶¹.

Budowa IndiaStack była przedsięwzięciem technicznym: polegała na stworzeniu systemu otwartych interfejsów programowania aplikacji (*application programming interface*, API), protokołów oraz platform. Przede wszystkim jednak stanowiła wyzwanie społeczne i logistyczne związane z włączaniem mieszkańców Indii w system. Zaangażowani w przedsięwzięcie wolontariusze

docierali do mieszkańców w odległych regionach kraju, asystując w tworzeniu elektronicznych dowodów tożsamości czy ucząc korzystania z funkcjonalności systemu. W efekcie IndiaStack to dziś ponad 1,3 miliarda tożsamości elektronicznych weryfikowanych dotąd w różnych celach ponad 63,6 miliardów razy¹⁶².

IndiaStack wskazywany jest często jako inspiracja w dążeniach do technologicznej suwerenności¹⁶³ nie tylko dla krajów globalnego Południa, ze względu na niewielki koszt uruchomienia systemu, lecz także dla globalnej Północy. Wprost odwołuje się do niego chociażby ruch EuroStack¹⁶⁴. Inspiracje płynące z Indii dotyczą na przykład pozytywnej roli partnerstw publiczno-prywatnych w inicjatywach na rzecz techsuwerenności; korzyści z istnienia bazowej, publicznej, relatywnie otwartej infrastruktury cyfrowej dla podmiotów prywatnych czy non-profit budujących własne produkty i usługi; roli standardów technicznych w budowaniu suwerenności technologicznej. **Inicjatywa ta stanowi jednak także źródło ostrzeżeń dla Europy.**

IndiaStack, ze względu na niewielki koszt uruchomienia systemu, wskazywany jest jako inspiracja również dla krajów globalnej Północy.

Camille Ford i współautorzy wskazują trzy główne punkty krytyki IndiaStacka¹⁶⁵. Po pierwsze, wątpliwości budzi bezpieczeństwo danych gromadzonych na masową skalę. Po drugie, krytycy wskazują na potencjał do nadużywania IndiaStacka w celach naruszania prywatności obywateli czy nawet masowej inwigilacji. Obawy te wzrosły w ostatnich latach wraz ze wzrostem autorytaryzmu rządu Narendry Modiego¹⁶⁶. **Z projektem Aadhaar od początku związane były kontrowersje dotyczące tego, czy mieszkańcy Indii na pewno świadomie zgadzają się na bycie włączonymi do systemu. Sąd Najwyższy tego kraju w 2018 r. uznał konstytucyjność inicjatywy, ograniczył jednak**

możliwość stawiania obywatelom wymogu posiadania elektronicznej tożsamości¹⁶⁷. Aktywiści wskazują jednak, że w praktyce prawo nie jest respektowane¹⁶⁸. Trzeci wątek w krytyce projektu IndiaStack dotyczy granic jego otwartości. Części systemu są zamknięte i kontrolowane w pełni przez administrację, co tylko zwiększa obawy o nadużycia ze strony władzy.

Przykład Indii to wreszcie lekcja o tym, że cyfrowe dobra publiczne same w sobie nie gwarantują rozwoju lokalnej branży technologicznej i mogą zostać wykorzystane do zdominowania rynku przez zagranicznych gigantów cyfrowych. System UPI służący pośredniczeniu w płatnościach okazał się żywną glebą do rozwoju usług Google oraz Walmarta¹⁶⁹. To jeden z powodów, dla których w Indiach trwa obecnie debata na temat nowego, inspirowanego europejskim DMA, prawa ochrony konkurencji na rynku cyfrowym¹⁷⁰. Jednocześnie jednak UPI stanowi zabezpieczenie dla mieszkańców Indii, gdyby firmy te zdecydowały się wycofać z kraju lub zaczęły im oferować gorsze warunki. Lukę po nich szybko zapełnią lokalne podmioty operujące na tej samej infrastrukturze.



BRAZYLIA

W ostatnim roku Brazylia stała się ważnym punktem odniesienia w dyskusjach dotyczących regulowania wielkich platform społecznościowych. Powodem był przede wszystkim głośny spór brazylijskiego Federalnego Sądu Najwyższego z Elonem Muskem. W październiku 2024 roku eskalował on do poziomu krótkotrwałej blokady portalu X w kraju i zajęcia majątku spółek związanych z miliarderem¹⁷¹.

Demokratyczny kraj wyłączający sądownie dostęp do platformy społecznościowej stanowił globalny precedens. Wywołał on w Europie debatę: czy działania te powinny zainspirować europejskich regulatorów, by nie obawiali się podobnych ruchów, czy też raczej są przestrogą przed sędziowskim aktywizmem.

Brazylia jest ciekawym przypadkiem do analizy także z innych powodów. Po pierwsze stanowi wzorcowy przykład kraju, na który wpłynął „efekt Brukseli”¹⁷². Brazylijscy legislatorzy starają się wprowadzić w kraju akty inspirowane DSA, DMA i aktem w sprawie sztucznej inteligencji. Napotykają jednak silny opór, także w postaci lobbingu. W konsekwencji sygnały płynące z Unii Europejskiej, która jest jakoby gotowa osłabić egzekwowanie cyfrowych praw, rezonują negatywnie w Brazylii¹⁷³. Ilustruje to geopolityczny aspekt techsuwerenności. **Paradoksalnie skutkiem zabiegów Europy o uniezależnianie się od Chin i USA nie jest izolacja na globalnej scenie politycznej, ale otwieranie nowych możliwości współpracy z krajami o podobnych ambicjach.**

Brazylia to wreszcie kolejny ciekawy punkt odniesienia dla projektów rozwoju publicznej infrastruktury cyfrowej – przede wszystkim za sprawą systemu Pix. Uruchomiony w 2020 roku przez Bank Centralny Brazylii, umożliwia bezpłatne dokonywanie transakcji online w realach. W świetle prac nad utworzeniem paneuropejskiego, suwerennego rozwiązania, które połączyłoby rozsiane inicjatywy lokalne takie jak polski Blik¹⁷⁴, doświadczenia Brazylii mogą być cenną inspiracją.



TAJWAN

Pierwszym skojarzeniem związanym z techsuwerennością i Tajwanem jest tamtejsza branża półprzewodnikowa. Historia jej rozwoju¹⁷⁵ jest niezwykle wartościowym źródłem wiedzy dla Europy starającej się zwiększyć udział w globalnej produkcji czipów. Relacje tajwańsko-chińskie to także żywy dowód, jak budować suwerenność mimo trudnej sytuacji geopolitycznej. Nic więc dziwnego, że nie tylko Bruksela, ale także poszczególne stolicy unijne (szczególnie Praga, Berlin i Warszawa¹⁷⁶) zabiegają o zacieśnianie stosunków z Tajpej w ramach strategii „friendshoringu”: budowy łańcuchów dostaw w oparciu o kraje najbliższe pod względem wartości i interesów, a niekoniecznie geograficznie¹⁷⁷.

Mniej znany aspekt polityki Tajwanu w zakresie nowych technologii stanowią osiągnięcia w **rozwijaniu cyfrowej demokracji**. Wiązane są głównie z postacią Audrey Tang, pierwszej w historii kraju ministry cyfryzacji, która objęła urząd w 2016 roku w następstwie między innymi studenckiej „Rewolucji słoneczników”. By zwiększyć możliwości społecznego angażowania się

obywateli w procesy demokratyczne, Tang, uznana programistka pracująca w przeszłości dla największych korporacji Doliny Krzemowej, oraz jej zespół opracowali lub wdrożyli szereg narzędzi w ramach inicjatywy vTaiwan¹⁷⁸. W procesie tym wypromowali między innymi platformę Pol.is służącą wypracowywaniu społecznych konsensusów. Na kanwie tajwańskich sukcesów platforma znalazła zastosowanie między innymi w Finlandii¹⁷⁹, Niemczech i Austrii¹⁸⁰. **UE i Polska, które mierzą się z kryzysem zaufania społecznego i rosnącą polaryzacją, powinny silniej zainteresować się doświadczeniami Tajwanu w cyfryzacji demokracji¹⁸¹.**



CHINY

Polityka cyfrowa chińskiego rządu stanowi dla Europy przede wszystkim negatywny punkt odniesienia. Unijne zabiegi techsuwerennościowe są w istotnej mierze reakcją na rosnący wpływ firm powiązanych z władzami w Pekinie, przede wszystkim w środkowo-wschodnim regionie Wspólnoty¹⁸². Od intensywnego zaangażowania Huawei i ZTE w budowę sieci 5G, przez rolę TikToka w europejskiej polityce, po agresywną ekspansję spółek e-handlu Temu, Shein i AliExpress, zakorzenienie się wielkiego chińskiego biznesu w Europie jest faktem, a skala zjawiska i jego konsekwencje są dopiero poddawane ocenie. We wrześniu ukazał się raport German Marshall Fund of the United States analizujący obecność chińskich podmiotów w niemieckim stosie technologicznym¹⁸³. Wreszcie, na podstawie tych doświadczeń, eksperci dostarczają wnioski na przyszłość: na przykład jak nie planować rozwoju sieci 6G¹⁸⁴.

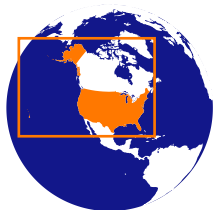
Mimo tych zastrzeżeń Unia Europejska stara się prowadzić cyfrowy dialog z Chinami¹⁸⁵. Uważnie przygląda się też działaniom rządu Xi Jinpinga dotyczącym technologicznej suwerenności rozumianej przez niego głównie jako *decoupling* od USA. Choć UE nie ma podobnych planów wobec transatlantyckiego (wciąż jeszcze) partnera, to stara się zmniejszyć zależność od niego. Czego w tym kontekście może się nauczyć od Chin?

Europejskie ośrodki analityczne najwięcej uwagi poświęcają temu, jak Pekin buduje własny stos technologiczny dla rozwoju sztucznej inteligencji¹⁸⁶. Temat ten eksploruje na przykład raport z lipca 2025 roku Mercator Institute for China Studies. Jak piszą we wstępie jego autorzy: „**analizowanie dążenia Chin do samowystarczalności w dziedzinie sztucznej inteligencji może (...) pomóc Europejczykom przewidzieć potencjalne problemy związane z tworzeniem EuroStacka**. Europa ma pewne strategiczne zasoby, w tym kluczowych dostawców sprzętu do produkcji półprzewodników i kilka znaczących start-upów LLM. Jednakże kontynent pozostaje w tyle pod względem rozwoju i wdrażania najbardziej zaawansowanych systemów sztucznej inteligencji”¹⁸⁷.

W konkluzjach zawierających sugestie dla europejskich polityków analitycy zwracają między innymi uwagę, że **Europa może nauczyć się od Chin wdrażania mniejszych, bardziej wyspecjalizowanych modeli SI (inspirowanych choćby DeepSeekiem, który wzbudził w Europie duży entuzjazm¹⁸⁸) w swojej silnej bazie przemysłowej¹⁸⁹**. Szczególnie interesującym przykładem wydaje się zacieśnianie relacji między branżami SI i motoryzacyjną¹⁹⁰. Zwracał na to uwagę Mario Draghi w przemówieniu na konferencji z okazji rocznicy publikacji sygnowanego swoim nazwiskiem raportu, mówiąc: „[s]ektorowe zastosowania sztucznej inteligencji są ważniejsze niż surowa

moc obliczeniowa superkomputerów. W tym zakresie Europa ma prawdziwą przewagę: jej firmy kontrolują ponad połowę światowego rynku rozwiązań w zakresie automatyki przemysłowej stanowiących fundament przemysłowej sztucznej inteligencji. Jednak tylko około 10 proc. firm produkcyjnych korzystało w zeszłym roku ze sztucznej inteligencji¹⁹¹. W najbliższym czasie okaże się, czy Bruksela uwzględni te i inne lekcje w będącej na finiszu prac strategii *Apply AI*.

Europa może wreszcie uczyć się także na błędach Chin. Mniej oczywiste przykłady to choćby kontrowersyjna polityka rozwoju regionalnego promująca konkurencję, a nie kooperację¹⁹², czy rosnące ryzyko nadpodaży mocy obliczeniowych w budowanych na masową skalę centrach danych¹⁹³. Choć ten drugi przypadek to dziś dla UE zagrożenie mocno potencjalne, to jednak warto przyglądać się także porażkom chińskiej ambicji, by czerpać korzyści z renty zapóźnienia.

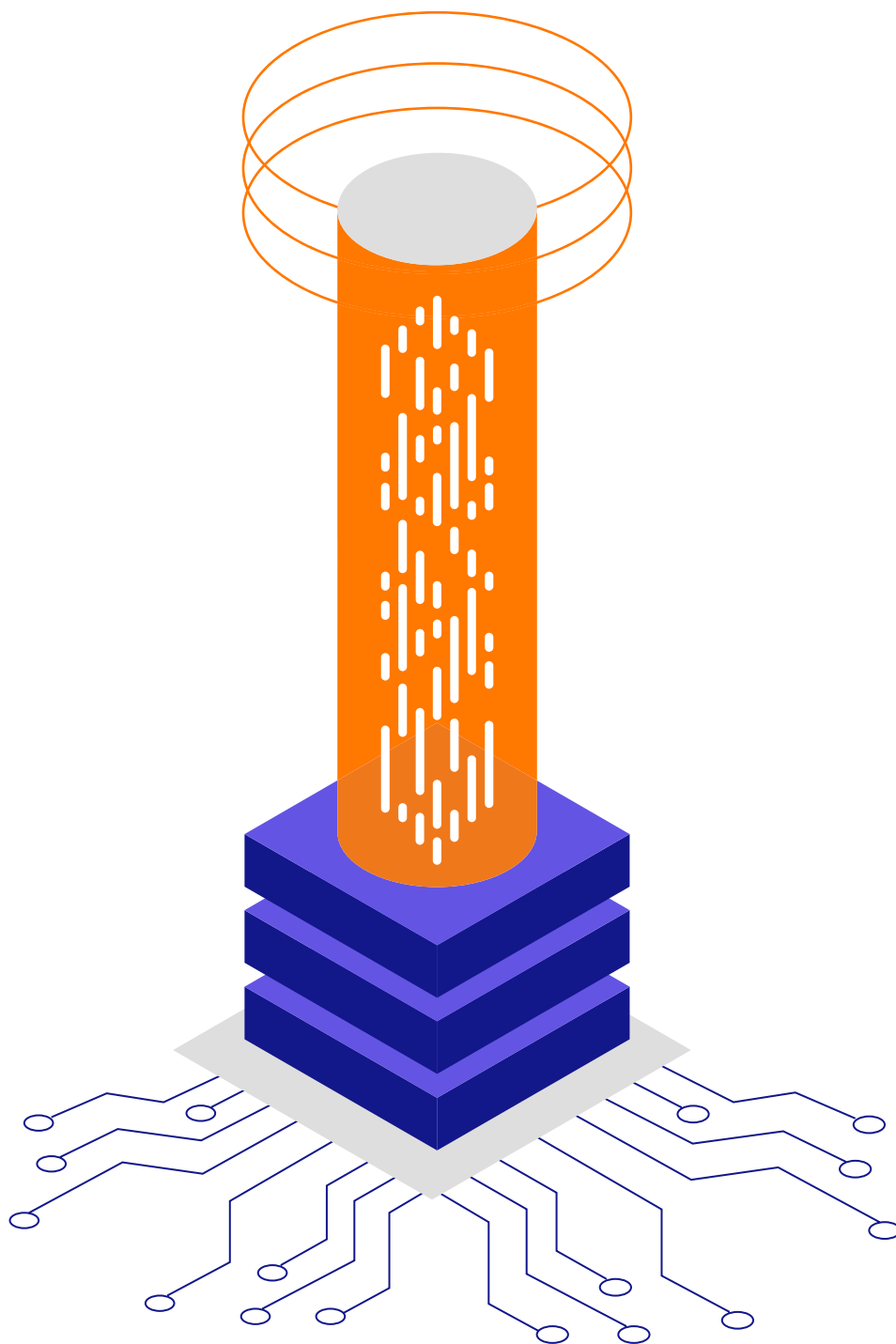


STANY ZJEDNOCZONE

USA są i długo jeszcze pozostaną najważniejszym punktem odniesienia dla polityk techsuwerennościowych w Europie. Parafrazując znany bon mot: gdy Waszyngton kicha, europejskie stolice dostają gorączki. Dobrym tego przykładem były reperkusje ogłoszenia w styczniu 2025 roku projektu Stargate. Inicjatywa pod patronatem Donalda Trumpa, z udziałem między innymi amerykańskich spółek OpenAI, Oracle i Nvidia, japońskiego funduszu Softbank oraz emirackiego MGX, ma do 2029 roku przeznaczyć około 500 miliardów dolarów na rozwój SI w USA¹⁹⁴. Najnowsze doniesienia amerykańskich mediów sugerują, że składane w styczniu deklaracje były na wyrost, a projekt mierzy się z poważnymi trudnościami wynikającymi ze sporów konsorcjantów¹⁹⁵. W międzyczasie zapowiedź zdążyła jednak wywołać panikę w Brukseli¹⁹⁶ i skłonić europejskich przywódców do licytacji na wielkość inwestycji w sztuczną inteligencję.

Stany nie muszą jednak inspirować Europy wyłącznie do reaktywnej polityki i wyścigu zbrojeń. W UE słychać coraz więcej głosów, że próby odtworzenia Doliny Krzemowej po drugiej stronie Atlantyku¹⁹⁷ czy deregulowania za amerykańskim przykładem branży sztucznej inteligencji¹⁹⁸ to przepis na katastrofę. Jednocześnie przykłady z USA nie muszą być tylko przestrogą dla Europy.

Kluczową lekcją płynącą ze Stanów jest znaczenie publicznych inwestycji w badania i innowacje oraz rozwój organizacji zdolnych nimi zarządzać¹⁹⁹. Za złoty standard wśród instytucji uważana jest legendarna Defence Advanced Research Projects Agency (DARPA), znana także jako ARPA, choć współcześnie zadania badawczo-rozwojowe realizuje w USA cały system agencji federalnych. Według najnowszych danych UNESCO wydatki na B+R stanowią około 3,6 proc. amerykańskiego PKB – a tylko 2,2 proc. PKB Unii Europejskiej. Nawet europejscy liderzy, jak Szwecja (3,4 proc.) czy Niemcy (3,1 proc.), ledwie zbliżają się do wyników Stanów. W odpowiedzi na trwające od dawna apele o stworzenie „europejskiej DARPA”²⁰⁰ Komisja Europejska zapowiedziała w strategii dla start-upów i scale-upów, że „rozszerzy zakres Europejskiej Rady ds. Innowacji oraz uprości jej zasady. EIC w większym stopniu skupi się na ukierunkowanym na wyzwania, etapowym finansowaniu innowacji wysokiego ryzyka poprzez wprowadzenie większej liczby procesów wzorowanych na praktykach ARPA”²⁰¹. Zarząd Europejskiej Rady ds. Innowacji apeluje jednak, że za tymi zmianami musi iść wzrost finansowania²⁰².



Rekomendacje

Analiza rozwoju idei techsuwerenności w Unii Europejskiej oraz lekcji płynących z różnych stron świata prowadzi do kilku ogólnych wniosków – rekomendacji dla decydentów z sektorów publicznego i prywatnego.

1

Idea techsuwerenności – polityki ograniczania zależności, budowy własnych kompetencji oraz mądrych partnerstw – powinna stać się strategiczną wytyczną dla Polski i Europy. Świadomość jej znaczenia i praktycznych sposobów realizowania musi wzrosnąć wśród wszystkich decydentów, bo technologia jest dziś wszechobecna. Przy wąskim definiowaniu problemu, w kategoriach dbania o konkretną infrastrukturę fizyczną czy ochrony danych, możliwe jest realizowanie jej przez pojedynczych, rozproszonych aktorów. Jednak szeroko zakrojona suwerenność wymaga współpracy i skoordynowanych działań. Powinny one całościowo obejmować stosy technologiczne, identyfikować ryzyka rozsiane w różnych rodzajach infrastruktury i wzmacniać różne typy odporności. Złożoność wyzwania może się wydawać paraliżująca, ale szerokie definiowanie go jest konieczne, by dążenia suwerennościowe nie były tylko działaniami pozornymi. Wreszcie, Europa powinna budować swoją techsuwerenność jako całość, starając się unikać pułapek narodowego izolacjonizmu, który osłabia jej potencjał.

2

Środki publiczne muszą popłynąć silniej do europejskich podmiotów. Po pierwsze oznacza to realizowanie zasady *Buy European*, a więc reformę zamówień publicznych i wprowadzenie klauzuli europejskiego pochodzenia do zakupów w sektorach kluczowych z perspektywy budowy lokalnego stosu technologicznego (od oprogramowania i usług cyfrowych po energię). Po drugie, wspieranie środkami publicznymi lokalnych (krajowych, unijnych) podmiotów powinno być priorytetem tam, gdzie proces decydowania o wyborze dostawców produktów i usług nie wymaga przetargów. Po trzecie wsparcie powinny odczuć także inicjatywy non-profit, jak choćby środowiska rozwijające rozwiązania *open source*, które są gotowe do wykorzystania w administracji czy szkolnictwie publicznym.

3

Europa musi zwiększyć i lepiej skoordynować wydatki na badania i rozwój. Innowacje są ich pochodną. Szeroko dyskutowana europejska luka innowacyjności ogranicza nie tylko wzrost konkurencyjności gospodarczej, ale również dokonywanie przełomowych odkryć czy tworzenie wynalazków. Silna baza badawczo-rozwojowa jest fundamentem techsuwerenności. Ostatnie dekady pokazały, że bez wsparcia i zachęt ze strony administracji sektor prywatny sam z siebie go nie postawi. Unijna strategia na rzecz start-upów i scale-upów zawiera ambitną mapę drogową dla promowania innowacyjności, między innymi poprzez *European Innovation Act*. Regulowaniu musi jednak towarzyszyć istotny wzrost wydatków publicznych przede wszystkim w takich krajach jak Hiszpania, Włochy czy Polska: dużych gospodarkach, które nie wykorzystują swojego potencjału.

4

Techsuwerenność musi być budowana na bazie silnej i konkurencyjnej gospodarki.

Tylko wtedy proces ten będzie naturalny i osadzony na trwałej podstawie. Dlatego UE i stolicy muszą zabiegać o stworzenie dobrego, stabilnego i przyjaznego otoczenia regulacyjnego i legislacyjnego z jasno nakreślonymi celami strategicznymi. Przy projektowaniu nowych przepisów i przeglądzie już przyjętych ważnym elementem procesu powinna być ocena, czy zwiększają bądź zmniejszają zależności zewnętrzne, szczególnie w kluczowych obszarach. Wysiłki nakierowane na tworzenie i wspieranie podmiotów europejskich nie mogą skutkować transferem kompetencji i kapitału poza UE, do krajów o lepszych warunkach rozwoju.

5

Decyzji dotyczących technologii nie może warunkować lęk przed ryzykiem.

Choć sugestia ta może się wydawać kontrintuicyjna w świetle uwag o deriskingu, to jednak przedstawiciele sektora publicznego często przyznają, że dalsze uzależnianie się od nie-suwerennych rozwiązań wynika często ze zbytnej zachowawczości. Wybór europejskiej alternatywy dla danego produktu czy usługi wymagać może odwagi, szczególnie, gdy wiąże się z decyzjami o dużych kwotach. Dotyczy to nie tylko sektora publicznego, ale i prywatnego. Kultura unikania ryzyka obecna choćby w europejskich regulacjach, choć co do zasady słuszna, może przyjmować formy patologiczne. Plany upraszczania prawa w Polsce i w UE mogą być okazją do zmierzenia się z tym problemem. Jego przejawem jest traktowanie ryzyk związanych z technologiami nie jako wyzwań, których należy być świadomym i z którymi można się mierzyć, lecz wyłącznie jako kłopotów do uniknięcia.

6

Techsuwerenność powinna stanowić środek do różnych celów.

Nie należy jej rozpatrywać jako celu samego w sobie, ale jako sposób zabezpieczania różnorodnych interesów publicznych i gospodarczych. W tym sensie może stanowić ścieżkę realizowania transformacyjnych polityk publicznych związanych ze sprawiedliwością społeczną, przeciwdziałaniem zmianom klimatu czy budowaniem odporności społecznej na różnorodne zagrożenia (wojenne, pandemiczne).

7

Infrastruktura krajowa i europejska muszą być chronione przed kryzysami.

Zasoby infrastrukturalne, takie jak sieci telekomunikacyjne, centra danych, ośrodki badawczo-rozwojowe czy produkcyjne, same w sobie nie gwarantują suwerenności, ale są dla niej bazą. Realizują swoje zadania w sytuacji kumulujących się zagrożeń: klimatycznych, kinetycznych, hybrydowych, militarnych. Dlatego też dążeniom do techsuwerenności muszą towarzyszyć starania o zabezpieczenie tej bazy przed zaburzeniami ciągłości działania. Powinny one przyjmować formę regulacji, spójnie wdrażanych w całej UE, oraz wsparcia finansowego przeznaczonego na doposażenie, modernizację lub wymianę kluczowych zasobów. Dbłość o bezpieczeństwo całego stosu technologicznego zgodnie z zasadą, że łańcuch jest tak silny, jak jego najsłabsze ogniwo, da techsuwerenności stabilny i bezpieczny fundament do rozwoju.

Bibliografia

- 1 Jakob Edler i in., Technology Sovereignty: From Demand to Concept, Research Report 02 / 2020 (Karlsruhe: Fraunhofer-Institut für System - und Innovationsforschung ISI, 2020), 10, <https://doi.org/10.24406/publica-fhg-300409>.
- 2 Paul Grant, „Technological sovereignty: forgotten factor in the ‘hi-tech’ razzamatazz”, Prometheus 1, nr 2 (1983): 239.
- 3 Ibid., 240.
- 4 Ibid., 261–63.
- 5 Ursula von der Leyen, „Von der Leyen: Nowa strategia cyfrowa da Unii technosuwerenność [OPINIA DLA DGP]”, Dziennik Gazeta Prawna, 19 lutego 2020, <https://www.gazetaprawna.pl/wiadomosci/artykuly/1454609,nowa-strategia-cyfrowa-da-unii-technosuwerennosc-von-der-leyen-dgp.html>.
- 6 Por. np. Jakob Edler i in., „Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means”, Research Policy 52, nr 6 (2023): 2, <https://doi.org/10.1016/j.respol.2023.104765>; Piotr Lewandowski, „Suwerenność technologiczna – teoretyczna i analityczna konceptualizacja pojęcia w obszarze badań społecznych”, Politeja: pismo Wydziału Studiów Międzynarodowych i Politycznych Uniwersytetu Jagiellońskiego Vol. 21, No. 3 (90) (2024): 28; 39–44, <https://doi.org/10.12797/Politeja.21.2024.90.11>.
- 7 Na ten temat np. Jeff Horwitz, Broken Code: Inside Facebook and the Fight to Expose Its Toxic Secrets (Random House, 2023); Kate Conger i Ryan Mac, Character Limit: How Elon Musk Destroyed Twitter (Penguin Press, 2024).
- 8 Jan J. Zygmuntowski, Kapitalizm sieci, wydanie I (Rozruch, 2020); Shoshana Zuboff, Wiek kapitalizmu inwigilacji: walka o przyszłość ludzkości na nowej granicy władzy, tłum. Alicja Unterschuetz (2019; wydanie I, Zysk i S-ka, 2022); Rebecca Giblin i Cory Doctorow, Chokepoint capitalism: how big tech and big content captured creative labor markets and how we'll win them back (Beacon Press, 2022).
- 9 Edler i in., „Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means”, 2.
- 10 Timo Seidl i Luuk Schmitz, „Moving on to not fall behind? Technological sovereignty and the ‘geo-dirigiste’ turn in EU industrial policy”, Journal of European Public Policy 31, nr 8 (2024): 2147–74, <https://doi.org/10.1080/13501763.2023.248204>.
- 11 Lewandowski, „Suwerenność technologiczna – teoretyczna i analityczna konceptualizacja pojęcia w obszarze badań społecznych”, 222.
- 12 Organization for Security and Co-operation in Europe, „What We Do”, Osce.Org, dostęp 9 września 2025, <https://www.osce.org/what-we-do>.
- 13 Por. np. Jakob Edler, „Chapter 8. Technology sovereignty of the EU: needs, concepts and pitfalls”, Science, research and innovation performance of the EU, 2024, przez Komisja Europejska i Dyrekcja Generalna ds. Badań Naukowych i Innowacji (Publications Office of the European Union, 2024), 428, <https://doi.org/doi/10.2777/965670>; Ignacy Świąćicki, „W kierunku suwerenności technologicznej”, Pomorski Thinkletter, nr 2 (21) (2025): 162, <https://www.kongresobywatelski.pl/pomorski-thinkletter/w-kierunku-suwerennosci-technologicznej/>.
- 14 Francesco Crespi i in., „European Technological Sovereignty: An Emerging Framework for Policy Strategy”, Intereconomics 56, nr 6 (2021): 348–54, <https://doi.org/10.1007/s10272-021-1013-6>.
- 15 Falkner i in., „Digital sovereignty – Rhetoric and reality”, 2102.
- 16 Patrik Hummel i in., „Data Sovereignty: A Review”, Big Data & Society 8, nr 1 (2021): 15, <https://doi.org/10.1177/2053951720982012>.
- 17 Cecilia Rikap, A progressive roadmap for expanding European digital sovereignty, FEPS Policy Brief (2025), <https://feeps-europe.eu/wp-content/uploads/2025/08/Digital-Sovereignty.pdf>.
- 18 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Trade Policy Review – An Open, Sustainable and Assertive Trade Policy (2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0066>.
- 19 Edler, „Chapter 8. Technology sovereignty of the EU: needs, concepts and pitfalls”, 433–34.

- 20 REPORT on European technological sovereignty and digital infrastructure (2025/2007(INI)) (European Parliament Committee on Industry, Research and Energy, 2025), https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.pdf; Charlotte Beaucillon i Sara Poli, „Special Focus on EU Strategic Autonomy and Technological Sovereignty: An Introduction”, *European Papers – A Journal on Law and Integration* 2023 8 (lipiec 2023): 411416, <https://doi.org/10.15166/2499-8249/663>.
- 21 Seidl i Schmitz, „Moving on to not fall behind?”; Sergio Mariotti, „“Open Strategic Autonomy” as an Industrial Policy Compass for the EU Competitiveness and Growth: The Good, the Bad, or the Ugly?”, *Journal of Industrial and Business Economics* 52, nr 1 (2025): 1-26, <https://doi.org/10.1007/s40812-024-00327-y>.
- 22 Komisja Europejska, „Updating the 2020 Industrial Strategy”, 5 maja 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1884.
- 23 Seidl i Schmitz, „Moving on to not fall behind?”, 2148-49.
- 24 Ibid., 2154.
- 25 WSPÓLNY KOMUNIKAT DO PARLAMENTU EUROPEJSKIEGO, RADY EUROPEJSKIEJ I RADY W SPRAWIE „EUROPEJSKIEJ STRATEGII BEZPIECZEŃSTWA GOSPODARCZEGO”, JOIN(2023) 20 final (2023), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52023JC0020>.
- 26 Emily Benson i in., „The Transatlantic Tech Clash: Will Europe “De-Risk” from the United States?”, Center for Strategic and International Studies (CSIS), 5 lutego 2025, <https://www.csis.org/analysis/transatlantic-tech-clash-will-europe-de-risk-united-states>.
- 27 Tim Rühlig i Maja Björk, What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe (The Swedish Institute of International Affairs, 2020).
- 28 Christoph March i Ina Schieferdecker, Technological Sovereignty as Ability, Not Autarky, Working Paper no. 9139 (CESifo Working Paper, 2021), <https://www.econstor.eu/handle/10419/236681>.
- 29 Ibid., 13.
- 30 Edler, „Chapter 8. Technology sovereignty of the EU: needs, concepts and pitfalls”, 433.
- 31 March i Schieferdecker, Technological Sovereignty as Ability, Not Autarky, 13-18.
- 32 Edler i in., Technology Sovereignty, 24.
- 33 Lukas Schaupp, „Decoding the Intersection of Trade and Security in the EU’s Anti-Coercion Instrument”, *European Foreign Affairs Review* 29, Issue 2 (2024): 156, <https://doi.org/10.54648/EERR2024006>.
- 34 Michał Woźniak, „Dlaczego wszystkie tajne służby nienawidzą Edwarda Snowdena. I za co my możemy mu być wdzięczni”, OKO.press, 17 czerwca 2023, <https://oko.press/dlaczego-wszystkie-tajne-sluzby-nienawidza-edwarda-snowdena-i-za-co-my-mozemy-byc-mu-wdzieczni>.
- 35 Wojciech Panek, „The Transfer of Personal Data from the European Union to the People’s Republic of China – the Influence on Consumer Rights of the Lack of Transparency in Data Transfers”, *Internetowy Kwartalnik Antymonopolowy i Regulacyjny* 14, nr 1 (2025): 81-95, <https://doi.org/10.7172/2299-5749.IKAR.1.14.5>.
- 36 Vili Lehdonvirta i in., „Weaponised Interdependence in a Bipolar World: How Economic Forces and Security Interests Shape the Global Reach of US and Chinese Cloud Data Centres”, *Review of International Political Economy*, 21 kwietnia 2025, 15, <https://doi.org/10.1080/09692290.2025.2489077>.
- 37 Synergy Research Group, „European Cloud Providers’ Local Market Share Now Holds Steady at 15%”, 24 lipca 2025, <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>.
- 38 Elena Sánchez Nicolas, „2013: Snowden was «wake-up Call» for GDPR”, *EUobserver*, 29 grudnia 2020, <https://euobserver.com/20th-anniversary/ardcd7bd7e>.
- 38 Foo Yun Chee i Sudip Kar-Gupta, „EU Court Backs Latest Data Transfer Deal Agreed by US and EU”, *Boards, Policy & Regulation*, Reuters, 3 września 2025, <https://www.reuters.com/sustainability/boards-policy-regulation/eu-court-backs-latest-data-transfer-deal-agreed-by-us-eu-2025-09-03/>.
- 40 noyb, „EU-US Data Transfers: First Reaction on «Latombe» Case”, *Noyb.Eu*, 3 września 2025, <https://noyb.eu/en/eu-us-data-transfers-first-reaction-latombe-case>.
- 41 Judson Althoff, „Announcing Comprehensive Sovereign Solutions Empowering European Organizations”, *The Official Microsoft Blog*, 16 czerwiec 2025, <https://blogs.microsoft.com/blog/2025/06/16/announcing-comprehensive-sovereign-solutions-empowering-european-organizations/>; Hayete Gallot, „Google Advances Sovereignty, Choice, and Security in the Cloud”, *Google Cloud Blog*, 21 maj 2025, <https://cloud.google.com/blog/products/identity-security/google-advances-sovereignty-choice-and-security-in-the-cloud>.

- 42 Synergy Research Group, „European Cloud Providers’ Local Market Share Now Holds Steady at 15%”.
- 43 Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism, First edition (PublicAffairs, 2013).
- 44 Rana Foroohar, „Year in a Word: Techlash”, 16 grudnia 2018, <https://www.ft.com/content/76578fba-fca1-11e8-ac-00-57a2a826423e>.
- 45 Ursula von der Leyen, „A Union that strives for more. My agenda for Europe”, 2019, 13, https://commission.europa.eu/document/download/063d44e9-04ed-4033-acf9-639ecb187e87_en.
- 46 Dan Milmo, „TikTok Fined €530m by Irish Regulator for Failing to Guarantee China Would Not Access User Data”, Technology, The Guardian, 2 maj 2025, <https://www.theguardian.com/technology/2025/may/02/tiktok-fined-530m-for-failing-to-protect-user-data-from-chinese-state>.
- 47 Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society, Cambridge Studies in European Law and Policy (Cambridge University Press, 2022), <https://doi.org/10.1017/9781009071215>.
- 48 Rada Europejska, „European Council meeting (19 October 2017) – Conclusions”, 19 października 2017, <https://www.consilium.europa.eu/media/21620/19-euco-final-conclusions-en.pdf>.
- 49 Wniosek DYREKTYWA RADY ustanawiająca przepisy dotyczące opodatkowania osób prawnych, których obecność na rynku cyfrowym jest znacząca, COM/2018/0147 final-2018/072 (CNS) (2018), <https://eur-lex.europa.eu/legal-content/PL/ALL/>; Wniosek DYREKTYWA RADY w sprawie wspólnego systemu podatku od usług cyfrowych pobieranego od przychodów wynikających ze świadczenia niektórych usług cyfrowych, COM/2018/0148 final-2018/073 (CNS) (2018), <https://eur-lex.europa.eu/legal-content/PL/ALL/>.
- 50 Jorge Valero, „The EU’s Digital Tax Is Dead, Long Live the OECD’s Plans”, Euractiv, 8 marca 2019, <https://www.euractiv.com/section/economy-jobs/news/the-eus-digital-tax-is-dead-long-live-the-oecd-plans/>.
- 51 Benoît Thieulin, Towards a European Digital Sovereignty Policy (Economic, Social and Environmental Council, 2019), 8.
- 52 Liz Alderman, „France Moves to Tax Tech Giants, Stoking Fight With White House”, Business, The New York Times, 11 lipca 2019, <https://www.nytimes.com/2019/07/11/business/france-digital-tax-tech-giants.html>.
- 53 Liz Alderman i in., „France and U.S. Move Toward Temporary Truce in Trade War”, Business, The New York Times, 21 stycznia 2020, <https://www.nytimes.com/2020/01/21/business/france-US-digital-tax.html>.
- 54 David Lawder i Leigh Thomas, „U.S. Drops Tariff Threat in Digital Tax Transition Deal with European Countries”, Europe, Reuters, 21 października 2021, <https://www.reuters.com/world/europe/european-countries-reach-digital-services-tax-deal-with-us-2021-10-21/>.
- 55 Jan J. Zygmuntowski i in., Podatek cyfrowy od gigantów. Ekspertyza w zakresie wprowadzenia w Polsce podatku cyfrowego (DST), no. 02/2020, Instrat Policy Paper (2020), https://instrat.pl/wp-content/uploads/2020/05/Podatek-cyfrowy-od-gigantow-Instrat-Policy-Paper-02_2020-1.pdf.
- 56 „Eksperci: potrzebujemy Polskiej Karty Suwerenności Cyfrowej”, PAP MediaRoom, 14 kwietnia 2020, <https://pap-mediroom.pl/biznes-i-finance/eksperci-potrzebujemy-polskiej-karty-suwerennosci-cyfrowej>.
- 57 Blanka Wawrzyniak i in., Polska suwerenna cyfrowo. Regulacje na rzecz sprawiedliwej i konkurencyjnej gospodarki cyfrowej, no. 06/2020, Instrat Policy Paper (Instrat, 2020), <https://instrat.pl/wp-content/uploads/2020/10/Polska-suwerenna-cyfrowo-Instrat.pdf>.
- 58 Projekt ustawy o podatku od niektórych usług cyfrowych i Funduszu Technologii Cyfrowych, No. 1376 (2020), 23, <https://orka.sejm.gov.pl/Druki9ka.nsf/0/CAA12BFAFD2D1850C125870B003960ED/%24File/1376.pdf>.
- 59 Michał Hetmański i in., Opodatkowanie działalności cyfrowej. Ekspertyza w zakresie wprowadzenia podatku cyfrowego w Polsce (Instrat, 2025).
- 60 „Polska potrzebuje suwerennej infrastruktury cyfrowej. Apelujemy do rządu”, Fundacja Panoptykon, 25 marca 2025, <https://panoptykon.org/infrastruktura-cyfrowa-apel-podatek-cyfrowy>.
- 61 Elżbieta Rutkowska, „Minister cyfryzacji Krzysztof Gawkowski: Wiemy, do kogo idziemy po pieniądze z podatku cyfrowego [WYWIAD]”, Dziennik Gazeta Prawna, 19 sierpnia 2025, <https://www.gazetaprawna.pl/firma-i-prawo/artykuly/9865032,wiemy-do-kogo-idziemy-po-pieniadze-z-podatku-cyfrowego-wywiad.html>.
- 62 Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, European Commission, „Industrial Alliances”, dostęp 10 września 2025, https://single-market-economy.ec.europa.eu/industry/industrial-alliances_en.
- 63 Ministerstwo Rozwoju i Technologii, „Mechanizm IPCEI – wspieramy politykę gospodarczą oraz politykę konkurencji UE”, 18 czerwca 2025, <https://www.gov.pl/web/rozwoj-technologie/mechanizm-ipcei-wspieramy-polityke-gospodarcza-oraz-polityke-konkurencji-ue>.

- 64 Juan Roch i Alvaro Oleart, „How ‘European sovereignty’ became mainstream: the geopoliticisation of the EU’s ‘sovereign turn’ by pro-EU executive actors”, *Journal of European Integration* 46, nr 4 (2024): 545–65, <https://doi.org/10.1080/07036337.2024.2326831>.
- 65 Jean-Claude Juncker, „CZAS EUROPEJSKIEJ SUWERENNOŚCI”, Komisja Europejska, 12 września 2018, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_5808.
- 66 „About the IPCEI – IPCEI on Microelectronics”, Ipcei-Me.Eu, dostęp 13 września 2025, <https://www.ipcei-me.eu/what-is/>.
- 67 „About IPCEI”, IPCEI Batteries, dostęp 13 września 2025, <https://www.ipcei-batteries.eu/about-ipcei>.
- 68 Von der Leyen, „A Union that strives for more. My agenda for Europe”, 13.
- 69 Jean-Pierre Darnis, European technological sovereignty: a response to the Covid-19 crisis?, no. 45/20, Note de la FRS (Fondation pour la recherche stratégique, 2020), <https://www.frstrategie.org/sites/default/files/documents/publications/notes/2020/202045.pdf>.
- 70 COMMISSION STAFF WORKING DOCUMENT: Strategic Dependencies and Capacities (2021), <https://eur-lex.europa.eu/legal-content/EN/TXT/>.
- 71 Aktualizacja nowej strategii przemysłowej z 2020 r. – tworzenie silniejszego jednolitego rynku sprzyjającego odbudowie Europy (2021), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52021DC0350>.
- 72 Plan działania na rzecz synergii między przemysłem cywilnym, obronnym i kosmicznym, COM(2021) 70 final (2021), <https://eur-lex.europa.eu/legal-content/pl/ALL/?uri=COM:2021:70:FIN>.
- 73 Ibid., 9.
- 74 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1781 z dnia 13 września 2023 r. w sprawie ustanowienia ram dotyczących środków na rzecz wzmocnienia europejskiego ekosystemu półprzewodników oraz zmiany rozporządzenia (UE) 2021/694 (akt w sprawie czipów) (Tekst mający znaczenie dla EOG), 229 OJ L (2023), <http://data.europa.eu/eli/reg/2023/1781/oj/pol>.
- 75 Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie” do 2030 r. (Tekst mający znaczenie dla EOG), 323 OJ L (2022), <http://data.europa.eu/eli/dec/2022/2481/oj/pol>.
- 76 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/795 z dnia 29 lutego 2024 r. w sprawie ustanowienia Platformy na rzecz Technologii Strategicznych dla Europy (STEP) oraz zmiany dyrektywy 2003/87/WE oraz rozporządzeń (UE) 2021/1058, (UE) 2021/1056, (UE) 2021/1057, (UE) nr 1303/2013, (UE) nr 223/2014, (UE) 2021/1060, (UE) 2021/523, (UE) 2021/695, (UE) 2021/697 i (UE) 2021/241, No. 2024/795 (2024), <http://data.europa.eu/eli/reg/2024/795/oj/pol>.
- 77 Guntram Wolff i in., The governance and funding of European rearmament, no. 15/2025, Policy Brief (Bruegel, 2025), https://www.bruegel.org/sites/default/files/2025-05/PB%2015%202025_0.pdf.
- 78 Sauli Niinistö, Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness (Komisja Europejska, 2024), 128.
- 79 Ulrike Franke, „Drones in Ukraine: Four Lessons for the West”, ECFR, 10 stycznia 2025, <https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west/>.
- 80 Jan Jęcz, Z góry lepiej widać. Perspektywy polskiego sektora obserwacji Ziemi (Polityka Insight, 2025), 10.
- 81 ICEYE, „ICEYE i SATIM zawiązują partnerstwo na rzecz nowych produktów do analizy obrazowań SAR wykorzystujących AI”, 10 lutego 2025, <https://www.iceye.com/pl-pl/press/press-releases/iceye-i-satim-zawiazuja-partnerstwo-na-rzecz-nowych-produktow-do-analizy-obrazowan-sar-wykorzystujacych-ai>.
- 82 „Helsing and ARX Robotics Announce Strategic Partnership”, Helsing, 9 września 2025, <https://helsing.ai/newsroom/helsing-and-arx-robotics-announce-strategic-partnership>.
- 83 Jan Jęcz, „Elon Musk zatrzymał atak ukraińskich dronów? Co ujawnia nowa biografia”, OKO.press, 11 września 2023, <https://oko.press/elon-musk-zatrzymal-atak-ukrainskich-dronow>.
- 84 Patricia Zengerle, „US Government Revokes Some Access to Satellite Imagery for Ukraine”, World, Reuters, 7 marca 2025, <https://www.reuters.com/world/us-aerospace-firm-maxar-disables-satellite-photos-ukraine-2025-03-07/>.
- 85 Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, JOIN(2020) 18 final (2020), 6, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52020JC0018>.
- 86 „How Does War in Ukraine Impact the EU’s Digital Sovereignty?”, EU Cyber Direct, 8 września 2022, <https://eucyber-direct.eu/blog/how-does-war-in-ukraine-impact-the-eu-s-digital-sovereignty>.
- 87 Jamila Boutemour i in., ENISA Threat Landscape 2025 (ENISA, 2025), 8, <https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf>.

- 88 Steven Lee Myers i in., „Russian Disinformation Campaigns Eluded Meta’s Efforts to Block Them”, *Business, The New York Times*, 17 stycznia 2025, <https://www.nytimes.com/2025/01/17/business/russia-disinformation-meta.html>.
- 89 Roland Hellberg i Martin Lundmark, Transformation in European Defence Supply Chains as Ukraine Conflict Fuels Demand | *Scandinavian Journal of Military Studies*, 2 styczeń 2025, <https://doi.org/10.31374/sjms.303>.
- 90 Nataliya Katser-Buchkovska, „The Future of Critical Raw Materials in Ukraine and the World”, *World Economic Forum*, 9 lipca 2024, <https://www.weforum.org/stories/2024/07/the-future-of-critical-raw-materials-how-ukraine-plays-a-strategic-role-in-global-supply-chains/>.
- 91 Niinistö, Safer Together: Strengthening Europe’s Civilian and Military Preparedness and Readiness, 96-100.
- 92 Enrico Letta, Much More than a Market – Speed, Security, Solidarity (2024), 59.
- 93 Mario Draghi, The future of European competitiveness. Part A: A competitiveness strategy for Europe (Komisja Europejska, 2024), 6.
- 94 Ibid., 24.
- 95 Mario Draghi, The Future of European Competitiveness. Part B: In-depth analysis and recommendations (Komisja Europejska, 2024), 77.
- 96 Draghi, The future of European competitiveness. Part A: A competitiveness strategy for Europe, 34.
- 97 Draghi, The Future of European Competitiveness. Part B: In-depth analysis and recommendations, 82-83.
- 98 Bertin Martens, „Draghi Disappoints on Digital”, *Bruegel*, 11 września 2024, <https://www.bruegel.org/first-glance/dra-ghi-disappoints-digital>.
- 99 Ursula von der Leyen, „Europe’s Choice. Political Guidelines for the Next European Commission 2024–2029”, 18 lipca 2024, 10, https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?file-name=Political%2525252520Guidelines%25252525202024-2029_EN.pdf.
- 100 Plan działania na rzecz kontynentu sztucznej inteligencji, COM/2025/165 final (2025), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52025DC0165>.
- 101 Draghi, The future of European competitiveness. Part A: A competitiveness strategy for Europe, 5.
- 102 Digital Markets Act. Preliminary remarks on certain designated gatekeepers’ compliance measures (European Tech Alliance, 2024), <https://eutechalliance.eu/wp-content/uploads/2024/04/EUTA-DMA-Concerns-on-gatekeepers-compliance-measures-May-2024.pdf>.
- 103 Jennifer Rankin, „Europe ‘Must Not Be Bullied’ by Trump and Musk on Tech Laws, NGOs Say”, *World News, The Guardian*, 29 stycznia 2025, <https://www.theguardian.com/world/2025/jan/29/europe-must-not-be-bullied-by-trump-and-musk-on-tech-laws-ngos-say>.
- 104 Polona Carr, Enforcing the Digital Services Act: State of Play, PE 766.256, Briefing (2024).
- 105 Stan cyfrowej dekady w 2024 r., COM/2024/260 final (2024), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52024DC0260>.
- 106 Zuzanna Warso i Meret Baumgartner, Putting Money Where Your Mouth Is? Insights into EU R&I Funding for Digital Technologies (critical infrastructure lab, 2025), 12, <https://doi.org/10.5281/zenodo.15263223>.
- 107 Free Software Foundation Europe, „European Commission Cuts Funding Support for Free Software Projects”, *European Digital Rights (EDRI)*, 20 sierpnia 2024, <https://edri.org/our-work/european-commission-cuts-funding-support-for-free-software-projects/>.
- 108 Komisja Europejska i in., Benchmarking the impact of the next generation internet initiative – Final study report (Publications Office of the European Union, 2024), <https://doi.org/doi/10.2759/062218>.
- 109 Francesca Bria, „The Quest for European Technological Sovereignty: Building the EuroStack | TechPolicy.Press”, *Tech Policy Press*, 15 października 2024, <https://techpolicy.press/the-quest-for-european-technological-sovereignty-building-the-eurostack>.
- 110 Mark Scott i Konstantinos Komaitis, „Reenvisioning Europe’s Digital Sovereignty”, *POLITICO*, 23 września 2024, <https://www.politico.eu/article/europe-ursula-von-der-leyen-tech-brussels-digital/>.
- 111 Aleksandra Wójtowicz, Przyszłość Rady ds. Handlu i Technologii za prezydentury Donalda Trumpa, no. 27, *Biuletyn PISM (Polski Instytut Spraw Międzynarodowych)*, 2025, <https://www.pism.pl/publikacje/przyszlosc-rady-ds-handlu-i-technologii-za-prezydentury-donald-trumpa>.
- 112 Alina Polyakova i in., „A European Tech Agenda 2.0”, *CEPA*, 21 listopada 2024, <https://cepa.org/article/a-european-tech-agenda-2-0/>.
- 113 Daniel Mügge, „The Trump Win and Its Lesson for EU Tech Policy”, *Euractiv*, 8 listopada 2024, <https://www.euractiv.com/section/tech/opinion/the-trump-win-and-its-lesson-for-eu-tech-policy/>.

- 114 J. D. Vance, „Remarks by the Vice President at the Artificial Intelligence Action Summit in Paris, France”, The American Presidency Project, 11 lutego 2025, <https://www.presidency.ucsb.edu/documents/remarks-the-vice-president-the-artificial-intelligence-action-summit-paris-france>.
- 115 Benedikt Franke, Munich Security Conference 2025. Speech by JD Vance and Selected Reactions, Selected Speeches held at the Munich Security Conference 2 (Mittler, 2025), https://securityconference.org/assets/02_Dokumente/01_Publikationen/2025/Selected_Key_Speeches_Vol_II/MS_C_Speeches_2025_Vol2_Ansicht_gek%C3%BCrzt.pdf.
- 116 The White House, „Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties”, The White House, 21 lutego 2025, <https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/>.
- 117 „EU Launches InvestAI Initiative to Mobilise €200 Billion”, European Commission, 11 lutego 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_467.
- 118 Francesca Bria i in., EuroStack – A European Alternative for Digital Sovereignty (Bertelsmann Stiftung, 2025), <https://www.bertelsmann-stiftung.de/doi/10.11586/2025006>.
- 119 Martin Hullin i Teresa Staiger, „EuroStack: The Urgency of Europe's Digital Independence”, BSt Europe, 18 marca 2025, <https://bst-europe.eu/competitiveness-innovation/eurostack-the-urgency-of-europes-digital-independence/>.
- 120 „Szef Google po spotkaniu z Tuskiem: podpisujemy memorandum ws. zastosowania AI”, Polska Agencja Prasowa, 13 lutego 2025, <https://www.pap.pl/aktualnosci/szef-google-po-spotkaniu-z-tuskiem-podpisujemy-memorandum-ws-zastosowania-ai>.
- 121 Anna Wittenberg, „Tusk ogłasza sukces. A naprawdę? Oddaje Google monopol na AI w Polsce”, Dziennik Gazeta Prawna, 13 lutego 2025, <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9738237,tusk-oglasza-sukces-a-naprawde-oddaje-google-monopol-na-ai-w-polsce.html>.
- 122 „D9+ Ministerial Declaration: Amsterdam Declaration”, 27 marca 2025, https://www.ceoe.es/sites/ceoe-corporativo/files/content/file/2025/04/02/104/_signatories_-draft-amsterdam-declaration-d9_-ministerial-meeting-27-march-2025-opgemaakt.pdf.
- 123 Théophane Hartmann, „European Industry Big Win: Germany, France Both Support Sovereign EU-Based Tech Infrastructure”, Euractiv, 10 kwietnia 2025, <https://www.euractiv.com/section/tech/news/european-industry-big-win-germany-france-both-support-sovereign-eu-based-tech-infrastructure/>.
- 124 REPORT on European technological sovereignty and digital infrastructure (2025/2007(INI)).
- 125 Jan Krewer, „Looking for an Exit: Europe's Way to Public Digital Infrastructures”, Tech Policy Press, 5 marca 2025, <https://techpolicy.press/looking-for-an-exit-europes-way-to-public-digital-infrastructures>.
- 126 Zuzanna Warso i Jan Krewer, Digital Commons as Providers of Public Digital Infrastructures (Open Future, 2024), 4.
- 127 Maximilian Henning, „Quartet of EU Countries to Cooperate on Building Sovereign Digital Infrastructure”, Euractiv, 9 lipca 2025, <https://www.euractiv.com/section/tech/news/quartet-of-eu-countries-to-cooperate-on-building-sovereign-digital-infrastructure/>.
- 128 Komisja Europejska, „IRIS2 | Secure Connectivity”, dostęp 16 września 2025, https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en.
- 129 Europejska strategia kwantowa, COM/2025/363 final (2025), <https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=celex:52025DC0363>.
- 130 Plixavra Vogiatzoglou i Joris van Hoboken, „The EU's Digital Sovereignty and Quantum Technologies: To What End?”, SSRN Scholarly Paper no. 5461374 (Social Science Research Network, 19 sierpnia 2025), <https://doi.org/10.2139/ssrn.5461374>.
- 131 Daniel Thomas, „Should Europe Wean Itself Off US Tech?”, BBC, 17 sierpnia 2025, <https://www.bbc.com/news/articles/c3dpr2zkny0o>.
- 132 Matheo Malik, „Les citoyens veulent-ils vraiment de la souveraineté numérique? 10 points sur une enquête mondiale”, Le Grand Continent, 25 września 2025, <https://legrandcontinent.eu/fr/2025/09/25/souverainete-technologique-10-points/>.
- 133 Seidl i Schmitz, „Moving on to not fall behind?”, 2167.
- 134 „Who We Are”, EuroStack, dostęp 15 września 2025, <https://eurostack.eu/who-we-are/>.
- 135 Edler i in., „Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means”, 6.
- 136 Max von Thun i Marietje Schaake, „Europe's Tech Sovereignty Demands More Than Competitiveness”, Project Syndicate, 11 kwietnia 2025, <https://www.project-syndicate.org/commentary/europe-misguided-fixation-on-enhancing-tech-competitiveness-by-marietje-schaake-and-max-von-thun-2025-04>.

- 137 Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie 2023/C 23/01, OJ C (2023), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ%3AJOC_2023_023_R_0001.
- 138 Kompas konkurencyjności dla UE, COM(2025) 30 final (2025), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52025DC0030>.
- 139 Unijna strategia na rzecz przedsiębiorstw typu start-up i scale-up, COM/2025/270 final (2025), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:52025DC0270>.
- 140 Warso i Krewer, Digital Commons as Providers of Public Digital Infrastructures, 8.
- 141 Rikap, A progressive roadmap for expanding European digital sovereignty, 14.
- 142 Bria i in., EuroStack – A European Alternative for Digital Sovereignty, 20.
- 143 Ibid., 20–21.
- 144 Np. Kai Zenner i in., „The European Way. A Blueprint for Reclaiming Our Digital Future”, SSRN Scholarly Paper no. 5251254 (Social Science Research Network, 12 maja 2025), 13, <https://doi.org/10.2139/ssrn.5251254>; Camille Ford i in., Building the European Digital Public Infrastructure: Rationale, Options, and Roadmap (Centre for European Policy Studies, 2025), 61.
- 145 Bria i in., EuroStack – A European Alternative for Digital Sovereignty, 30–31.
- 146 Cristina Caffarra i in., Deploying the EuroStack: What’s needed now. (2025), 8–9; Zenner i in., „The European Way. A Blueprint for Reclaiming Our Digital Future”, 17.
- 147 Bria i in., EuroStack – A European Alternative for Digital Sovereignty, 107.
- 148 Bert Hubert, „But how to get to that European cloud?”, Posts, Bert Hubert’s writings, 17 marca 2025, <https://berthub.eu/articles/posts/now-how-to-get-that-european-cloud/>.
- 149 Draghi, The future of European competitiveness. Part A: A competitiveness strategy for Europe, 63.
- 150 J. Scott Marcus, „It’s Finally Time to Leverage Pension Funds to Foster EU Productivity and Benefit Pensioners”, CEPS, 10 lutego 2025, <https://www.ceps.eu/its-finally-time-to-leverage-pension-funds-to-foster-eu-productivity-and-benefit-pensioners/>.
- 151 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS State of the Digital Decade 2025: Keep building the EU’s sovereignty and digital future, COM(2025) 290 final (2025), 11, <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52025DC0290>.
- 152 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS State of the Digital Decade 2025.
- 153 Catherine Bracy, World Eaters: How Venture Capital Is Cannibalizing the Economy, 1st ed (Penguin Publishing Group, 2025).
- 154 Bria i in., EuroStack – A European Alternative for Digital Sovereignty, 104.
- 155 REPORT on European technological sovereignty and digital infrastructure (2025/2007(INI)).
- 156 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Establishing the European Competitiveness Fund (‘ECF’), Including the Specific Programme for Defence Research and Innovation Activities, Repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/697, (EU) 2021/783, Repealing Provisions of Regulations (EU) 2021/696, (EU) 2023/588, and Amending Regulation (EU) [EDIP], COM/2025/555 final (2025), <https://eur-lex.europa.eu/legal-content/EN/TXT/>.
- 157 Zuzanna Warso i Aditya Singh, From Public Investment to Public Value. An Agenda for Digital Sovereignty, no. 9, OpenFuture Policy Brief (Open Future, 2025).
- 158 Mariana Mazzucato, Mission Economy: A Moonshot Guide to Changing Capitalism (Penguin UK, 2021).
- 159 Edler i in., „Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means”, 7; Mariotti, „“Open Strategic Autonomy” as an Industrial Policy Compass for the EU Competitiveness and Growth”, 9.
- 160 Vivek Raghavan i in., „India Stack – Digital Infrastructure as Public Good”, Communications of the ACM 62, nr 11 (2019): 76–81, <https://doi.org/10.1145/3355625>; Aaryaman Vir i Rahul Sanghi, „The Internet Country”, Tigerfeathers, 19 września 2020, <https://www.tigerfeathers.in/p/the-internet-country>.
- 161 Raghavan i in., „India Stack – Digital Infrastructure as Public Good”.
- 162 „India Stack | Identity”, dostęp 17 września 2025, <https://indiastack.org/identity.html>.
- 163 Chloe Teevan i in., From India Stack to EuroStack: Reconciling approaches to sovereign digital infrastructure, 2025, <https://ecdpm.org/application/files/2117/3874/5474/From-India-Stack-to-EuroStack-Reconciling-Approaches-Sovereign-Digital-Infrastructure-ECDPM-Discussion-Paper-384.pdf>.

- 164 Robin Berjon i in., „#EUROSTACK: EUROPEAN STRATEGIC SOVEREIGN DIGITAL INFRASTRUCTURES”, styczeń 2025, 8, https://euro-stack.eu/wp-content/uploads/2025/01/EuroStack-Report_Digital-A4_Latest_v6-2.pdf; Bria i in., EuroStack – A European Alternative for Digital Sovereignty, 95.
- 165 Ford i in., Building the European Digital Public Infrastructure: Rationale, Options, and Roadmap, 14–15.
- 166 J. P. Singh, „India Stack: Authority and Innovation in a New Financial Infrastructure”, The Cambridge Global Handbook of Financial Infrastructure, red. Barbara Brandl i in. (Cambridge University Press, 2025), 344, <https://doi.org/10.1017/9781009428118.031>.
- 167 Aadhaar: India Top Court Upholds World’s Largest Biometric Scheme, 26 września 2018, <https://www.bbc.com/news/world-asia-india-44777787>.
- 168 Kiran Jonnalagadda, „Life without Aadhaar”, Deccan Herald, 21 września 2024, <https://www.deccanherald.com/india/life-without-aadhaar-3200235>.
- 169 Nilesh Christopher, „How Google, Facebook and Walmart Stole Paytm’s Fintech Crown in India”, Rest of World, 17 sierpnia 2021, <https://restofworld.org/2021/indias-paytm-goes-public-in-the-shadow-of-facebook-google-and-walmart/>.
- 170 Navneet Sharma, „The Government’s Pivot or Retreat on the Digital Competition Bill? – A Critical Reflection”, MEDIANAMA, 16 sierpnia 2025, <https://www.medianama.com/2025/08/223-india-digital-competition-bill-2024-withdrawal/>.
- 171 Tom Phillips, „Brazil Lifts Ban on X after Elon Musk Complies with Court Demands”, Technology, The Guardian, 8 października 2024, <https://www.theguardian.com/technology/2024/oct/08/musks-x-reinstated-in-brazil-after-complying-with-supreme-court-demands>.
- 172 Anu Bradford, The Brussels effect: how the European Union rules the world (Oxford University Press, 2020).
- 173 Miguel Otero-Iglesias i Gonzalo Rodríguez, „From Brussels to Brasilia: Regulatory Inspiration or Isolation?”, 7 kwietnia 2025, <https://www.ie.edu/insights/articles/from-brussels-to-brasil-ia-regulatory-inspiration-or-isolation/>.
- 174 „EuroPA and EPI Confirm Commitment to Expand Sovereign Pan-European Payments with a Hub Model”, EPI Company, 2 września 2025, <https://epicompany.eu/media-insights/europa-and-epi-confirm-commitment-to-expand-sovereign-pan-european-payments-with-a-hub-model>.
- 175 Mateus Lee i in., „The Competitiveness and Future Challenge of the Taiwan Semiconductors Industry”, Technology Rivalry Between the USA and China, red. Peter C.Y. Chow (Springer Nature Switzerland, 2024), https://doi.org/10.1007/978-3-031-76169-0_6.
- 176 Paulina Uznańska, Bridging the Gap: Enhancing CEE-Taiwan Collaboration in the Semiconductor Sector (Casimir Pulaski Foundation, 2024).
- 177 Yu-Ning Chiu, „Taiwan Under the US-EU Strategic Realignment: Supply Chain Resilience, Technological Decoupling and Sustainable Futures”, Global Taiwan Brief 10, nr 5 (2025): 3–6.
- 178 Carl Miller, „Taiwan Is Making Democracy Work Again. It’s Time We Paid Attention”, Tags, Wired, 26 listopada 2019, <https://www.wired.com/story/taiwan-democracy-social-media/>.
- 179 „Polis Platform Experiments”, Sitra, b.d., dostęp 19 września 2025, <https://www.sitra.fi/en/projects/polis-platform-experiments/>.
- 180 „The Computational Democracy Project”, dostęp 19 września 2025, <https://compdemocracy.org/Case-studies/>.
- 181 Ming-sho Ho, Exploring Worldwide Democratic Innovations – A Case Study of Taiwan (European Democracy Hub, 2022).
- 182 Marta Makowska, China’s Digital Authoritarianism vs. EU Technological Sovereignty: The Impact on Central and Eastern Europe (Council on Foreign Relations, 2022); Sylwia Czubkowska, Chińczycy trzymają nas mocno: pierwsze śledztwo o tym, jak Chiny kolonizują Europę, w tym Polskę, wydanie I (Znak Litera Nova, 2022).
- 183 Sharinee L. Jagtiani, Risky Configuration China’s Footprint in Germany’s Technology Stack (German Marshall Fund of the United States Technology Program, 2025), <https://www.gmfus.org/sites/default/files/2025-09/Germany%20Tech%20Stack.pdf>.
- 184 Tim Nicholas Rühlig, The “Huawei Saga” in Europe Revisited German Lessons for the Rollout of 6G, no. 187, Notes Du Cerfa (Ifri, 2025).
- 185 „Komisja i Chiny prowadzą drugi dialog cyfrowy wysokiego szczebla”, Komisja Europejska, 18 września 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4488.
- 186 Alicia García-Herrero i Pauline Weil, Lessons for Europe from China’s Quest for Semiconductor Self-Reliance, no. 19/22 (Bruegel, 2022); Wendy Chang i in., China’s Drive Toward Self-Reliance in Artificial Intelligence (MERICS | Mercator Institute for China Studies, 2025).
- 187 Chang i in., China’s Drive Toward Self-Reliance in Artificial Intelligence, 5–6.

- 188 Pieter Haeck, „Europe’s AI Hopes Rebound after DeepSeek Success”, POLITICO, 29 stycznia 2025, <https://www.politico.eu/article/europe-ai-scene-hope-china-deepseek-ai-model-r1-success/>.
- 189 Chang i in., China’s Drive Toward Self-Reliance in Artificial Intelligence, 21.
- 190 Charlie Campbell, „How China’s EV Boom Powers Its Tech Rise”, TIME, 29 maja 2025, <https://time.com/7288660/shift-east-china-electric-vehicles-economy-technology-trump-tariffs-ai/>.
- 191 Mario Draghi, „Keynote speech”, conference paper presented one year after the Draghi Report, Bruksela, 16 września 2025, https://commission.europa.eu/document/download/0951a4ff-cd1a-4ea3-bc1d-f603decc1ed9_en?filename=Draghi_Speech_High_Level_Conference_One_Year_After.pdf.
- 192 Saverio Barabuffi i in., „The »picking the fittest« approach and spatial dynamics in China’s artificial intelligence regional development”, Papers in Regional Science 104, nr 3 (2025): 100096, <https://doi.org/10.1016/j.pirs.2025.100096>.
- 193 „China Plans Network to Sell Surplus Computing Power in Crackdown on Data Centre Glut”, Technology, Reuters, 24 lipca 2025, <https://www.reuters.com/technology/china-plans-network-sell-surplus-computing-power-crackdown-data-centre-glut-2025-07-24/>.
- 194 „Ogłaszamy The Stargate Project”, OpenAI, 21 stycznia 2025, <https://openai.com/pl-PL/index/announcing-the-stargate-project/>.
- 195 Eliot Brown i Berber Jin, „Exclusive | SoftBank and OpenAI’s \$500 Billion AI Project Struggles to Get Off Ground”, The Wall Street Journal, 21 lipca 2025, <https://www.wsj.com/tech/ai/softbank-openai-a3dc57b4>.
- 196 Pieter Haeck, „Trump’s \$500B AI Plan Is ‘Slap’ in the Face for Europe”, POLITICO, 22 stycznia 2025, <https://www.politico.eu/article/us-500-ai-europe-donald-trump-global-leadership-eu-social-media-china/>.
- 197 Marietje Schaake, „How Should Europe Build Its Own Silicon Valley?”, 7 listopada 2024, <https://www.ft.com/content/5c-49d2a9-4dc4-4fd1-b1bf-0e35cb8a4f11>.
- 198 J. B. Branch i in., „The Trump AI Action Plan Is Deregulation Framed as Innovation”, Tech Policy Press, 30 lipca 2025, <https://techpolicy.press/the-trump-ai-action-plan-is-deregulation-framed-as-innovation>.
- 199 Gary Clyde Hufbauer i Euijin Jung, Scoring 50 Years of US Industrial Policy, 1970–2020, PIIE Briefing nos. 21–5 (Peterson Institute for International Economics, 2021), <https://www.piie.com/sites/default/files/documents/piieb21-5.pdf>; Alessio Terzi i in., Industrial Policy for the 21st Century: Lessons from the Past., no. 157, Discussion Paper (Komisja Europejska, 2022), 9–12, <https://data.europa.eu/doi/10.2765/538421>; Draghi, The future of European competitiveness. Part A: A competitiveness strategy for Europe, 29.
- 200 Lars Frølund i Fiona Murray, „Can Europe Really Build Its Own DARPA?”, Project Syndicate, 24 października 2024, <https://www.project-syndicate.org/commentary/european-darpa-could-boost-innovation-if-implemented-correctly-by-lars-fr-lund-and-fiona-murray-1-2024-10>.
- 201 Unijna strategia na rzecz przedsiębiorstw typu start-up i scale-up, 11.
- 202 European Innovation Council and SMEs Executive Agency, „European Innovation Council Board Calls for EIC’s Expanded Mission and Increased Budget to Boost Europe’s Deep Tech Leadership”, European Innovation Council, 1 lipca 2025, https://eic.ec.europa.eu/news/european-innovation-council-board-calls-eics-expanded-mission-and-increased-budget-boost-europes-2025-07-01_en.

