PARP
Grupa PFR

Monitoring cyfryzacji

Czerwiec 2026

Monitoring cyfryzacji: czerwiec 2026

Autorzy: Marcin Woźny i Krzysztof Kardaszewicz

Centrum Analiz i Strategii, Polska Agencja Rozwoju Przedsiębiorczości

Niniejsze opracowanie jest pierwszym materiałem przygotowanym w ramach nowej serii wydawniczej PARP pt. „Monitoring Cyfryzacji”. Publikowane co kwartał raporty mają na celu analizę wybranych trendów w cyfryzacji.

Kontakt w sprawie Raportu: analizy@parp.gov.pl

Spis treści

Wstęp

W ostatnich miesiącach dynamiczny rozwój cyfryzacji coraz wyraźniej uwidacznia napięcie między postępem technologicznym a rosnącą podatnością państw i przedsiębiorstw na zagrożenia cybernetyczne. Wyścig technologiczny wokół AI, chmury, półprzewodników i analityki danych sprawił, że cyberbezpieczeństwo przestało być postrzegane wyłącznie jako kwestia techniczna, a stało się istotnym elementem polityki przemysłowej, bezpieczeństwa narodowego i rywalizacji geopolitycznej. Coraz większego znaczenia nabiera również pojęcie „suwerenności cyfrowej". W świetle tych zmian i podejmowanych działań przedstawiamy przegląd wybranych trendów w ramach bieżącego *Monitoringu Cyfryzacji*.

Niniejsze opracowanie jest pierwszym w nowej, wydawanej kwartalnie, serii wydawniczej PARP pt. „Monitoring Cyfryzacji". Będziemy wdzięczni za wszelkie uwagi, które pomogą w doskonaleniu kolejnych edycji raportu (analizy@parp.gov.pl).

Nowa optyka cyberbezpieczeństwa

Pod wpływem rozwoju sztucznej inteligencji zmienia się zakres, częstotliwość i głębia cyfrowych zagrożeń. Najnowsze publikacje badaczy z firmy Google DeepMind wskazują, że obecne **systemy nadzoru nad sztuczną inteligencją nie nadążają za tempem jej rozwoju** (moc obliczeniowa modeli AI rośnie w tempie około 10x rocznie), a zaawansowane modele tej firmy nie są już definiowane jako bezpieczne i zaufane. W odpowiedzi, badacze przygotowali nowe założenia monitorowania sztucznej inteligencji („AI Control Roadmap") jednocześnie otwarcie przyznając, że obecnie wysuwane ostrzeżenia są marginalizowane przez decydentów[1,2].

Dostępne narzędzia AI już teraz ułatwiają i automatyzują działania potrzebne do przeprowadzenia ataku, a każdy incydent może potencjalnie sparaliżować szereg powiązanych ze sobą instytucji. W ubiegłym roku, w Polsce oficjalnie odnotowano 272 tysiące incydentów cyberbezpieczeństwa, co oznacza przyrost o 144%[3].

W rezultacie cyberbezpieczeństwo w coraz większym stopniu ujmowane jest jako element **wspólnego ekosystemu**, a nie jedynie odporności poszczególnych podmiotów i przedsiębiorstw. Szczególne znaczenie przypisuje się najsłabszym ogniwom w łańcuchu bezpieczeństwa, takim jak podwykonawcy czy dostawcy usług zewnętrznych, którzy często nie posiadają odpowiednich zabezpieczeń ani zasobów i kompetencji niezbędnych do ich rozwinięcia[4, 5].

[1] https://storage.googleapis.com/deepmind-media/DeepMind.com/Blog/securing-the-future-of-ai-agents/gdm-ai-control-roadmap.pdf
[2] https://cyfrowa.rp.pl/ai/art44659851-doktryna-wewnetrznego-wroga-dolina-krzemowa-przestaje-ufac-ai
[3] https://samorzad.gov.pl/web/gov/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025?utm
[4] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

Jest to kluczowy aspekt pod kątem działalności MŚP oraz różnic w zasobach i kompetencjach obserwowanych pomiędzy przedsiębiorstwami. Jak wynika z dostępnych badań, choć rośnie świadomość zagrożeń i wdrażane są kolejne unijne oraz krajowe regulacje mające dostosować wymogi do zmieniającego się krajobrazu cyberbezpieczeństwa[6], to możliwości i tempo wdrażania wymaganych rozwiązań są istotnie zróżnicowane w zależności od sektora działalności i rozmiaru firmy. Z dostępnych badań wynika, że 77% polskich firm przeznacza na cyberbezpieczeństwo poniżej 50 000 zł rocznie (w tym 37% poniżej 10 000 zł)[7]. Jedynie nieco ponad 30% badanych przedsiębiorstw prowadzi monitoring cyberzagrożeń i posiada scenariusz postępowania w przypadku wystąpienia incydentu. Podobny odsetek ma wypracowane procedury konieczne do spełnienia wymogów dyrektywy NIS2, wdrażanej w ramach znowelizowanej ustawy o Krajowym Systemie Cyberbezpieczeństwa[8].

W rezultacie obserwujemy narastający **dług bezpieczeństwa**, sytuację, w której tempo innowacji technologicznych przewyższa realną zdolność organizacji do modernizacji istniejącej infrastruktury oraz wdrażania odpowiednich mechanizmów bezpieczeństwa. Pod tym względem istotnym wyzwaniem jest również względnie **niski poziom kompetencji** cyfrowych w Polsce, które kształtują ogólne postrzeganie technologii oraz ich bezpieczeństwa i mają realny wpływ na skuteczność wdrożenia wprowadzanych przepisów i rozwiązań. Według dostępnych danych, podstawowe kompetencje cyfrowe w Polsce są jednymi z niżej ocenianych w Europie (posiada je 50,4% Polaków, przy unijnej średniej 60,4%), a brak zaufania do nowych technologii oraz ich bezpiecznego wykorzystania jest jedną z barier ograniczających zastosowanie w przedsiębiorstwach[9,10,11,12].

Przy obecnym tempie zmian, realnym wyzwaniem staje się kwestia narastającego **wykluczenia cyfrowego** i potencjalnych społecznych kosztów cyfryzacji gospodarki – między innymi ze względu na fałszywe treści i kampanie informacyjne generowane z pomocą sztucznej inteligencji, które sprawiają, że coraz trudniej weryfikować autentyczność informacji[13].

---

[5] Przykładem zmieniającego się podejścia jest również projekt Glasswing, zainicjowany przez firmę Anthropic, która udostępniła swój zaawansowany model AI firmom rozwijającym krytyczne oprogramowanie w celu wyszukiwania i naprawiania luk bezpieczeństwa (https://www.anthropic.com/glasswing). W podobny sposób, firma OpenAI udostępniła wybranym podmiotom narzędzie GTP 5.5 Cyber – korzysta z niego m.in. NASK (https://www.rp.pl/biznes/art44749231-polska-uzyskala-dostep-do-poteznej-broni-ai).

[6] https://gdpr.pl/ai-cyberbezpieczenstwo-i-odpornosc-cyfrowa-najwazniejsze-regulacje-ue-i-polski-czesc-i

[7] https://crn.pl/aktualnosci/77-proc-polskich-firm-wydaje-na-cyberbezpieczenstwo-najwyzej-50-tys-zl-rocznie/?utm

[8] https://pro.rp.pl/raporty-ekonomiczne/art43099091-polskie-firmy-zyja-w-iluzji-cyberbezpieczenstwa?utm

[9] https://digital-strategy.ec.europa.eu/en/factpages/poland-2025-digital-decade-country-report?utm

[10] https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2026-closing-structural-gaps-and-mobilising-investments-2030-and-beyond

[11] https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-zmieniajacej-uchwale-w-sprawie-ustanowienia-programu-rzadowego-pod-nazwa-program-rozwoju-kompetencji-cyfrowych

[12] https://www.parp.gov.pl/component/publications/publication/survey-report-global-entrepreneurship-monitor-poland-2025

[13] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

Dlatego obok rozwoju instytucji, procedur i infrastruktury, kluczowym wyzwaniem dla cyfryzacji i cyberbezpieczeństwa pozostanie element zaufania społecznego – zarówno dla bezpiecznego wykorzystania samych technologii (przykładowo, na zaufaniu opiera się powszechne stosowanie cyfrowych płatności), jak też weryfikacji i sprawnego przepływu spójnych i wiarygodnych informacji[14].

Suwerenność technologiczna

Zmiana myślenia o cyberbezpieczeństwie jest blisko powiązana z rosnącym znaczeniem suwerenności technologicznej, rozumianej przede wszystkim jako możliwość kontroli kluczowych zasobów (infrastruktura, technologie, dane) oraz ich zależności od zagranicznych dostawców i ograniczenia ryzyka zakłóceń lub utraty autonomii decyzyjnej. W coraz większym stopniu, państwa dokonują ponownej oceny swojej **zależności technologicznej** od zagranicznych dostawców i globalnych łańcuchów dostaw [15].

Głębia i znaczenie tych zależności są widoczne w narastającej rywalizacji pomiędzy USA i Chinami, w ramach której zaczęto zdecydowanie ograniczać np. wykorzystanie amerykańskich technologii w Chinach, oraz eksport zaawansowanych półprzewodników (do Chin), lub metali ziem rzadkich (do USA). Najnowszym obostrzeniem ze strony USA jest rozszerzenie kontroli eksportowych wobec zaawansowanego modelu AI firmy Anthropic – w praktyce blokując dostęp i wykorzystanie zagranicznym użytkownikom[16,17,18]. Ruch był przynajmniej częściowo podyktowany narastającymi obawami o „adversarial model distillation" – wykorzystanie przez Chiny dostępnych na rynku modeli AI amerykańskich firm jako bazy do wypracowania własnych, tańszych rozwiązań[19]. Z kolei w Chinach wprowadzane są rygorystyczne przepisy dotyczące wykorzystania i bezpieczeństwa danych (w tym w produktach takich jak inteligentne samochody)[20], ale również kontrole zagranicznych wyjazdów dla kluczowych specjalistów zajmujących się rozwojem sztucznej inteligencji[21].

---

[14] W kontroli narastającej dezinformacji ma za zadanie pomóc wdrażany właśnie w Polsce Digital Services Act, który wprowadza dla platform internetowych obowiązki większej przejrzystości i skuteczniejsze mechanizmy zgłaszania oraz usuwania nielegalnych treści. Akt ustala również wymogi dotyczące analizowania i ograniczania systemowych zagrożeń, takich jak algorytmiczne wzmacnianie fałszywych informacji, oraz możliwości nakładania sankcji za niewywiązywanie się z tych obowiązków.

[15] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

[16] https://www.anthropic.com/news/securing-america-s-compute-advantage-anthropic-s-position-on-the-diffusion-rule?aff=47lw0&utm

[17] https://www.reuters.com/technology/us-blocks-foreign-access-anthropics-most-advanced-ai-models-axios-reports-2026-06-13/?utm

[18] Należy odnotować, że w lipcu, po kilku tygodniach negocjacji z firmą Anthropic, administracja USA zdecydowała się na ponowne udostępnienie modeli AI zagranicznym użytkownikom. Dostępny model Fable 5 obecnie nie odpowiada jednak na pytania dotyczące cyberbezpieczeństwa i biologii. https://cyfrowa.rp.pl/ai/art44746621-usa-wycofaly-blokade-na-potezna-ai-anthropic-wraca-do-gry

[19] https://www.whitehouse.gov/wp-content/uploads/2026/04/NSTM-4.pdf

[20] https://www.osw.waw.pl/pl/publikacje/raport-osw/2025-12-17/smartfony-na-kolkach

[21] https://www.reuters.com/world/asia-pacific/china-restricts-overseas-travel-top-ai-talent-alibaba-deepseek-bloomberg-news-2026-05-26/?utm

Suwerenność technologiczna jest również kluczowym elementem działań Unii Europejskiej i państw członkowskich. W dostępnych analizach podkreśla się, że obecnie ponad 80% produktów, usług i własności intelektualnej w sektorze cyfrowym w krajach europejskich pochodzi spoza UE, w szczególności z USA. W Polsce wykazano deficyt w handlu produktami cyfrowymi wynoszący 45 mld zł, zaznaczając, że pod koniec obecnej dekady, produkty cyfrowe będą stanowić już blisko 10% całego importu. Jednocześnie 56% Polaków uważa, że suwerenność technologiczna ma duże lub bardzo duże znaczenie, a 71% jest gotowych zapłacić większą cenę za korzystanie z rodzimych rozwiązań.

Ograniczenie obecnej zależności technologicznej staje się niezbędne dla stabilności ekonomicznej, bezpieczeństwa i długoterminowej konkurencyjności Europy. Kluczowe stają się inwestycje kapitałowe w lokalną infrastrukturę i rozwiązania technologiczne oraz ochrona danych konsumentów oraz przedsiębiorców. Kolejne państwa – jak Dania, Francja, Niemcy – podejmują też działania na rzecz rozwoju usług „open source" i budowania niezależności od korporacyjnych monopoli i zależności od produktów oferowanych przez prywatne firmy (ryzyko tzw. vendor lock-in)[22].

W kontekście obecnych działań, Komisja Europejska opublikowała w czerwcu **pakiet na rzecz suwerenności cyfrowej**, mający na celu wsparcie rozwoju nowych technologii w oparciu o zaawansowane półprzewodniki, usługi chmurowe, sztuczną inteligencję oraz niezbędną infrastrukturę obliczeniową i zasoby energetyczne.

Europejski Pakiet Suwerenności Cyfrowej składa się z dwóch propozycji legislacyjnych: Chips Act 2.0 i Cloud and AI Development Act – a także Open Source Strategy i Strategic Roadmap for Digitalisation and AI in Energy. Dokumenty te zostaną opisane poniżej.

Europejski Pakiet Suwerenności Cyfrowej

Chips Act 2.0[23]

WPROWADZENIE

Pierwotny akt w sprawie chipów (Chips Act) stanowił pierwszą skoordynowaną odpowiedź UE na kluczowe słabe punkty w globalnym łańcuchu dostaw półprzewodników. Pomógł on zmobilizować ponad 52 mld EUR w postaci inwestycji publicznych i prywatnych, stworzył szacunkowo 46 000 bezpośrednich i pośrednich miejsc pracy oraz wzmocnił europejski potencjał badawczo-innowacyjny w dziedzinie półprzewodników.

Mimo tego postępu, UE pozostaje zależna od krajów trzecich w kluczowych obszarach, takich jak produkcja zaawansowanych układów scalonych czy projektowanie półprzewodników.

Globalny rynek półprzewodników również gwałtownie się rozwija. Oczekuje się, że do 2030 r. osiągnie on wartość 1,37 bln EUR, a komponenty związane ze sztuczną inteligencją będą

[22] https://digitalpoland.org/publikacje/pobierz?id=3fd02f02-bed7-45cf-a29e-6908ac83f16e
[23] https://digital-strategy.ec.europa.eu/en/library/proposal-chips-act-20

napędzać około 70% tego wzrostu. Chips Act 2.0 ma na celu zapewnienie, że Europa zdobędzie większy udział w tej szansie, przy jednoczesnym wzmocnieniu obszarów, w których już teraz się wyróżniamy[24].

GŁÓWNE POSTANOWIENIA

Pierwszym ogólnym celem rozporządzenia jest zapewnienie warunków niezbędnych dla konkurencyjności i zdolności innowacyjnych Unii w dziedzinie technologii półprzewodnikowych oraz zapewnienie przystosowania się przemysłu do zmian strukturalnych.

Drugim ogólnym celem, jest zwiększenie gotowości na wypadek kryzysu w celu zapewnienia UE bezpieczeństwa dostaw, a tym samym usprawnienie funkcjonowania rynku wewnętrznego poprzez ustanowienie jednolitych unijnych ram prawnych na rzecz zwiększenia odporności i dostępności w Unii w dziedzinie technologii półprzewodnikowych.

CHIPS FOR EUROPE INITIATIVE 2.0

W przeciwieństwie do pierwszej wersji aktu, która skupiała się głównie na dotowaniu fabryk (podaż), wersja 2.0 kładzie nacisk na to, aby europejski przemysł realnie kupował i wdrażał rodzime technologie. Służyć temu mają nowe mechanizmy:

- **Grand Challenges:** Projekty ukierunkowane na rozwój chipów o kluczowym znaczeniu komercyjnym i strategicznym dla UE, ze szczególnym uwzględnieniem chipów do sztucznej inteligencji.
- **Demand Accelerators:** Komisja i państwa członkowskie będą stymulować wykorzystanie półprzewodników zaprojektowanych lub wyprodukowanych w Unii, w szczególności na kluczowych rynkach, takich jak rynek usług w chmurze, motoryzacyjny, lotniczy, telekomunikacyjny, obronny oraz w stosownych przypadkach, na innych rynkach.

Inicjatywa rozszerza wsparcie finansowe i badawcze o sektory, które zadecydują o przyszłej suwerenności technologicznej Europy. Obok tradycyjnych procesorów, priorytetem stają się:

- Zaawansowane układy zorientowane na AI,
- Fotonika i zintegrowane obwody fotoniczne,
- Chipy kwantowe,
- Zaawansowane techniki pakowania układów scalonych.

Chips for Europe Initiative 2.0 utrzymuje wsparcie dla istniejących już linii pilotażowych i Centrów Kompetencji (European network of competence centres in semiconductors), ale tworzy dla nich strukturalne ścieżki komercjalizacji. Chodzi o to, aby startupy, firmy typu *scale-up* oraz MŚP mogły łatwiej i taniej testować swoje projekty na liniach pilotażowych, a następnie szybko wdrażać je do masowej produkcji.

[24] https://digital-strategy.ec.europa.eu/en/policies/chips-act-2

BEZPIECZEŃSTWO DOSTAW I POPYTU

Projekt legislacji wprowadza do porządku prawnego zrewidowaną procedurę przyznawania statusu Projektu Strategicznego (First-of-a-Kind Strategic Project). Aby podmiot gospodarczy mógł ubiegać się o ten status, inwestycja musi spełnić rygorystyczne kryteria prawne:

- Projekt musi wprowadzać na rynek unijny zdolności produkcyjne, które dotychczas w UE nie istniały;
- Wnioskodawca musi prawnie zobowiązać się, że w sytuacji kryzysowej priorytetowo obsłuży zamówienia unijne;
- Inwestycja nie może naruszać zasad równej konkurencji na rynku wewnętrznym, a państwo członkowskie wnioskujące o status dla projektu musi wykazać pozytywny wpływ na unijny łańcuch dostaw.

Kluczową nowością legislacyjną jest nałożenie na państwa członkowskie ustawowego obowiązku traktowania Projektów Strategicznych jako inwestycji nadrzędnego interesu publicznego oraz bezpieczeństwa publicznego. Wprowadza to następujące skutki prawne:

- Państwa członkowskie są prawnie zobowiązane do zakończenia wszystkich procedur administracyjnych (w tym ocen oddziaływania na środowisko, pozwoleń budowlanych i zintegrowanych) w ściśle określonym, skróconym okienku czasowym do 12 miesięcy;
- Nadanie statusu Projektu Strategicznego stanowi prawną podstawę do uproszczonej i przyspieszonej notyfikacji pomocy publicznej przed Komisją Europejską, umożliwiając państwom dotowanie do 100% luki finansowej inwestycji.

Ustanowione zostają nowe ramy prawne dla tworzenia transgranicznych klastrów przemysłowych (European Semiconductor Regions of Excellence). Przepisy te dają regionom spełniającym kryteria prawo do ubiegania się o dedykowane pakiety finansowe z funduszy strukturalnych na rozwój infrastruktury i programów edukacyjnych (zwalczanie deficytu kadr), a także znoszą wybrane bariery regulacyjne w przepływie zasobów i inżynierów między tymi regionami.

Projekt legislacji wprowadza obligatoryjny system monitorowania sektora półprzewodników.

- Państwa członkowskie są prawnie zobligowane do stałego monitorowania kondycji finansowej i logistycznej przedsiębiorstw z sektora półprzewodników na swoim terenie;
- W przypadku wykrycia anomalii rynkowych lub zagrożenia geopolitycznego, Komisja Europejska zyskuje uprawnienie prawne do nakazania kluczowym graczom rynkowym ujawnienia poufnych danych handlowych (struktury mocy produkcyjnych, stanów magazynowych, łańcuchów dostawców). Odmowa przekazania danych lub podanie informacji nieprawdziwych skutkuje sankcjami finansowymi.

W wypadku zidentyfikowania poważnych problemów w dostawach półprzewodników może zostać ogłoszony stan kryzysu, który uprawnia centralne organa Unii do sterowania dostawami wewnętrznymi i zewnętrznymi tak aby zapewnić dostawy do krytycznych zastosowań (zamówienia priorytetowe u dostawców wewnętrznych, centralizacja zakupów zewnętrznych w imieniu krajów członkowskich).

ZARZĄDZANIE

Rozporządzenie formalnie powołuje do życia European Semiconductor Board (ESB) jako stały organ doradczy i decyzyjny o charakterze instytucjonalnym.

- W skład Rady wchodzą wysocy rangą przedstawiciele państw członkowskich oraz Komisji Europejskiej (która przewodniczy obradom).
- ESB posiada prawnie zdefiniowany mandat do:
    - Opiniowania i rekomendowania wniosków o nadanie statusu Projektu Strategicznego;
    - Koordynowania działań państw członkowskich w zakresie monitorowania łańcuchów dostaw;
    - Uruchamiania procedur dyplomacji półprzewodnikowej (współpraca i umowy międzynarodowe z państwami trzecimi, np. USA, Tajwan, Korea Płd.).

Każde państwo członkowskie ma obowiązek wyznaczyć co najmniej jeden krajowy organ właściwy za wdrożenie i stosowanie rozporządzenia na swoim terytorium. W przypadku powołania większej liczby takich organów konieczne jest jasne rozdzielenie ich kompetencji oraz zapewnienie efektywnej współpracy, w tym przy wyznaczaniu jednego krajowego punktu kontaktowego.

Cloud and AI Development Act[25]

WPROWADZENIE

Cloud and AI Development Act (CADA) to kluczowa unijna regulacja, której głównym celem jest zbudowanie niezależności i konkurencyjności Europy w obszarze chmury obliczeniowej oraz infrastruktury dla sztucznej inteligencji.

„Obecny krajobraz w obszarze chmury i sztucznej inteligencji charakteryzuje się wyraźną zależnością od ograniczonej puli dostawców z krajów trzecich. Choć unijny rynek usług przetwarzania w chmurze odnotowuje znaczny wzrost, udział w rynku dostawców z UE spadł z 29% w 2017 roku do 15% w 2022 roku i od tamtego czasu pozostaje w stagnacji[26]".

Ustawa ta ma za zadanie uniezależnić Europę od dominacji amerykańskich i azjatyckich gigantów technologicznych (tzw. hyperscalers), gwarantując, że dane europejskich obywateli i firm są przetwarzane w bezpieczny i suwerenny sposób.

[25] https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada
[26] Cloud and AI Development Act

PRZEPISY OGÓLNE

Pierwszym ogólnym celem rozporządzenia jest zapewnienie warunków niezbędnych dla konkurencyjności i zdolności innowacyjnych unijnego ekosystemu chmury i sztucznej inteligencji.

Drugim ogólnym celem jest usprawnienie funkcjonowania jednolitego rynku poprzez ustanowienie jednolitych unijnych ram prawnych na rzecz zwiększenia odporności i strategicznej autonomii Unii w dziedzinie technologii chmurowych i sztucznej inteligencji.

Szczegółowe cele przedstawione w dokumencie zakładają:

1) potrojenie mocy obliczeniowych europejskich centrów danych do 2030 r. oraz osiągnięcie poziomu odpowiadającego europejskiemu zapotrzebowaniu do 2035 r.;

2) stworzenie warunków umożliwiających stosowne inwestycje – do 2030 potencjalni operatorzy centrów danych, mają być w stanie uzyskać wszystkie konieczne zezwolenia do budowy i prowadzenia działalności w maksymalnie 18 miesięcy (w tym zapewnienie wymaganej energii i łączności);

3) zwiększenie udziału w rynku usług chmurowych przez europejskie podmioty, zwłaszcza w celu ograniczenia zależności UE od zewnętrznych dostawców; przewiduje się m.in. wspólne zamówienia publiczne oraz preferencje dla europejskich dostawców, startupów i rozwiązań open source.

4) zapewnienie niezależnych usług chmurowych i AI dla podmiotów w sektorze publicznym UE, na podstawie własnych rozwiązań będących podstawą cyberbezpieczeństwa i odporności cyfrowej.

Nowe regulacje mają umożliwić przede wszystkim szybsze i spójne działania w oparciu o jednolity zestaw kryteriów wykorzystanych do audytu i weryfikacji suwerenności usług chmurowych. W związku z tym, dokument zakłada dalszą pracę nad stworzeniem europejskiego certyfikatu cyberbezpieczeństwa dla usług chmurowych (EUCS). Wreszcie, dokument ma stanowić rozwinięcie już obowiązujących aktów prawnych (jak np. NIS2, lub Cybersecurity Act), kładąc nacisk na rozwój wykorzystania technologii oraz ich suwerenność.

DZIAŁALNOŚĆ BADAWCZA, ROZWOJOWA I WDROŻENIOWA NA RZECZ EKOSYSTEMU CHMURY I AI

Inicjatywy Przewodnie w dziedzinie Chmury i AI (Cloud and AI Leadership Initiatives) mają na celu promowanie badań, innowacji oraz budowę wielkoskalowego potencjału w całym unijnym ekosystemie cyfrowym. Cel ten realizowany jest poprzez rozwijanie energooszczędnych technologii centrów danych, budowę autonomicznych systemów chmurowych oraz przyspieszenie rozwoju zaawansowanych modeli sztucznej inteligencji (w tym AI fizycznej i przemysłowej). Dodatkowo program dąży do wzmocnienia odporności infrastruktury oraz stymulowania popytu i wdrażania rozwiązań chmurowych oraz modeli AI zarówno w sektorze prywatnym, jak i publicznym.

Na państwa członkowskie nakładany jest obowiązek powołania **Centrów AI,** które mają bazować na strukturze Europejskich Hubów Innowacji Cyfrowych (EDIH). Ich głównym celem jest przyspieszenie cyfryzacji i powszechnego wdrażania technologii chmurowych oraz sztucznej inteligencji na poziomie lokalnym, ze szczególnym uwzględnieniem MŚP i sektora publicznego. Do konkretnych zadań Centrów należy łączenie organizacji z unijnymi dostawcami technologii, zapewnianie szkoleń i przekwalifikowania kadr, ułatwianie transferu wiedzy między regionami oraz wspieranie rozwoju startupów akademickich.

Ponadto nakładany jest obowiązek ustanowienia krajowych strategii chmurowych i AI. Strategie te mają być regularnie rewidowane co trzy lata na podstawie osiągniętych wskaźników.

Ustanawiane są rygorystyczne kryteria, na podstawie których Komisja Europejska może nadać konkretnemu projektowi status „priorytetowego projektu w dziedzinie zaawansowanej sztucznej inteligencji" (*frontier AI priority project*). Projekty o statusie priorytetowym będą miały uprzywilejowany dostęp do unijnych zasobów obliczeniowych.

ZASOBY CENTRÓW DANYCH

Na państwa członkowskie nakładany jest obowiązek identyfikacji i wyznaczenia na swoim terytorium specjalnych „stref akceleracji" (*data centre acceleration zones*), dedykowanych budowie i modernizacji infrastruktury obliczeniowej. Zobowiązuje się państwa do powołania jednego okienka (*single information points*) dla operatorów centrów danych. Punkt ten koordynuje i integruje całość procedur informacyjnych. Centra danych w strefach akceleracji powinny być traktowane jako projekty strategiczne. Procedura wydawania pozwoleń dla projektów centrów danych realizowanych w strefach akceleracji nie powinna przekraczać 12 miesięcy.

Ustanawia się mechanizm składania wniosków i przyznawania przez Komisję Europejską statusu „Strategicznego Projektu Centrum Danych" (*data centre strategic project*) dla inwestycji wprowadzających przełomowe innowacje w zakresie zrównoważonego rozwoju i efektywności energetycznej.

Komisja Europejska przyznaje sobie mandat do prowadzenia stałego nadzoru i monitoringu dostępnych mocy obliczeniowych w UE (w tym infrastruktury brzegowej), poziomu popytu rynkowego oraz wielkości luki wydajnościowej (*capacity gap*).

AUTONOMIA

Wprowadza się do porządku prawnego formalną strukturę czterech poziomów suwerenności chmurowej (*Union assurance levels 1 to 4*) o szczegółowo określonych kryteriach. Dla najniższego poziomu zapewnienia suwerenności (Poziom 1) wprowadza uproszczoną procedurę polegającą na samodzielnym przeprowadzeniu i udokumentowaniu oceny zgodności przez dostawcę. Do certyfikacji na wyższe poziomy wymagany jest oficjalny audyt.

Na Komisję Europejską nakłada się obowiązek prowadzenia publicznego, centralnego rejestru wszystkich usług chmurowych, które pomyślnie przeszły certyfikację na poziomach 1-4.

Definiuje się ramy odpowiedzialności cywilnej i administracyjnej dostawców chmur za naruszenie wymogów suwerenności, w tym zasady rekompensat dla podmiotów, których dane ucierpiały w wyniku naruszenia.

Każde państwo członkowskie musi powołać lub wskazać istniejący urząd jako krajowy organ właściwy odpowiedzialny za egzekwowanie przepisów aktu CADA. Nadaje się tym organom szerokie uprawnienia kontrolne, śledcze, prawo do nakładania natychmiastowych nakazów naprawczych i nakładania kar.

Nakłada się na państwa członkowskie i podmioty unijne obowiązek przeprowadzania ocen ryzyka w celu określenia, które zadania sektora publicznego i infrastruktury krytycznej wymagają stosowania określonych poziomów suwerenności chmurowej. W przypadku stwierdzenia konieczności migracji danych, proces ten musi zostać sfinalizowany w terminie nieprzekraczającym 12 miesięcy. Komisja Europejska może wydawać akty wykonawcze określające standardy i poziomy suwerenności dla konkretnych działań publicznych.

Akt definiuje zasady udzielania zamówień publicznych na usługi chmurowe i systemy AI przeznaczone do wyłącznego użytku instytucji zamawiających. Zobowiązuje administrację publiczną do uwzględniania kryteriów strategicznej autonomii, bezpieczeństwa danych i odporności na prawo państw trzecich, a także zakazuje zakupu usług niespełniających wymaganych certyfikatów w obszarach wrażliwych. Nakłada się też na instytucje zamawiające państw członkowskich obowiązek stosowania kryteriów unijnej wartości dodanej podczas zamówień publicznych na usługi chmurowe i systemy AI.

Ustanawia się Europejską Federację Chmur Sektora Publicznego (EuroCloud Federation). EuroCloud Federation stanowi kluczowy element unijnej strategii mającej na celu optymalizację cyfrowej infrastruktury publicznej oraz wzmocnienie suwerenności technologicznej Europy. Ta innowacyjna struktura została zaprojektowana jako bezpieczny, zintegrowany i zdecentralizowany ekosystem chmurowy, dedykowany wyłącznie dla administracji rządowej, samorządowej oraz instytucji i agencji Unii Europejskiej.

Podmioty publiczne decydują o chęci przystąpienia do tego wspólnego projektu, składając odpowiedni wniosek do Komisji Europejskiej. Głównym założeniem systemu jest umożliwienie bezpiecznego współdzielenia nadwyżek zasobów obliczeniowych i pojemności centrów danych, którymi dysponują poszczególne państwa. Wiele nowoczesnych publicznych ośrodków IT nie wykorzystuje w pełni swoich mocy przerobowych, podczas gdy mniejsze urzędy lub kraje o niższym stopniu zaawansowania cyfrowego zmagają się z brakiem infrastruktury. Federacja rozwiązuje ten problem, pozwalając na optymalne gospodarowanie zasobami w skali całej Wspólnoty.

Wszelkie koszty operacyjne, techniczne oraz wydatki związane z prowadzeniem platformy koordynującej wymianę są pokrywane przez uczestników federacji na zasadzie prostego zwrotu kosztów.

W ramach tego samego aktu prawnego, kolejnym istotnym filarem cyfrowej transformacji jest wprowadzenie mechanizmów wspólnych zamówień publicznych na zaawansowane usługi cyfrowe. Mechanizm ten opiera się na przyznaniu Komisji Europejskiej uprawnień do przeprowadzania wspólnych postępowań o udzielenie zamówienia publicznego na usługi przetwarzania w chmurze oraz systemy sztucznej inteligencji. Procedury te są realizowane na rzecz i w imieniu unijnych instytucji, organów i agencji, a także zainteresowanych podmiotów sektora publicznego z państw członkowskich oraz wybranych organizacji partnerskich.

Podobnie jak w przypadku federacji chmurowej, kluczowym elementem tego systemu jest zapewnienie jego finansowej samowystarczalności bez obciążania budżetu ogólnego. W związku z tym wprowadzono system opłat pobieranych od instytucji zamawiających, które decydują się na udział we wspólnych zamówieniach. Opłaty te są kalkulowane w sposób przejrzysty i proporcjonalny, a ich jedynym celem jest zrekompensowanie realnych kosztów operacyjnych i administracyjnych ponoszonych przez Komisję Europejską przy przygotowaniu i obsłudze tych zaawansowanych procedur zakupowych.

Kolejnym filarem unijnego aktu jest szerokie promowanie otwartości technologicznej oraz wprowadzenie zasady pierwszeństwa otwartego oprogramowania (*Open Source First*).

Wdrażanie tej strategii opiera się na nałożeniu na instytucje Unii Europejskiej oraz podmioty sektora publicznego w państwach członkowskich wyraźnego obowiązku dawania pierwszeństwa rozwiązaniom o otwartym kodzie źródłowym przed oprogramowaniem o charakterze zamkniętym (własnościowym). Co więcej, ramy te wprowadzają konkretne wymagania dotyczące dzielenia się oprogramowaniem, które zostało stworzone przez administrację publiczną lub na jej bezpośrednie zamówienie. Nowo powstały kod ma być udostępniany w sposób umożliwiający jego łatwe, ponowne wykorzystanie przez inne urzędy i instytucje na terenie całej Wspólnoty.

Aby ułatwić ten proces i uczynić go w pełni praktycznym, Komisja Europejska została zobowiązana do stworzenia i stałego prowadzenia oficjalnego, ogólnoeuropejskiego Katalogu Rozwiązań Open Source. Narzędzie to ma służyć jako centralna baza sprawdzonych, bezpiecznych i gotowych do wdrożenia aplikacji oraz systemów dla sektora publicznego. Całość struktur wspierających open source spina mechanizm tworzenia wyspecjalizowanych Biur ds. Programów Otwartego Oprogramowania (*Open Source Programme Offices*). Ta skoordynowana sieć biur w państwach członkowskich ma zapewniać wsparcie doradcze, techniczne oraz dbać o prawidłowe standardy wdrażania otwartych technologii w codziennej pracy administracji publicznej.

Open Source Strategy[27]

POTENCJAŁ RYNKOWY I BARIERY ROZWOJU OPEN SOURCE

Europa posiada unikalny potencjał – jest domem dla silnej i tętniącej życiem społeczności ponad 3 milionów twórców otwartego oprogramowania. Model open source pozwala na drastyczne obniżenie kosztów technologii, redukcję zjawiska uzależnienia od jednego dostawcy (*vendor lock-in*) oraz zapewnia unikalną transparentność z perspektywy cyberbezpieczeństwa (otwarty kod umożliwia publiczny audyt i wykrywanie podatności).

Mimo to, UE wydaje obecnie około 264 mld EUR rocznie, w większości na amerykańskie, zamknięte produkty własnościowe IT. Co więcej, blisko połowa commitów kodu w Europie pochodzi z małych firm (poniżej 50 pracowników), które zderzają się z barierami w dostępie do zamówień publicznych, niską rozpoznawalnością marki i trudnościami z kapitałem na skalowanie działalności. Dotychczasowe unijne wsparcie finansowe jest rozproszone i pozbawione strategicznego nastawienia na długofalowe utrzymanie i stabilność społeczności.

CZTERY FILARY OPERACYJNE STRATEGII

W celu eliminacji barier i stymulowania wzrostu, strategia definiuje cztery główne cele realizowane przez skoordynowane działania podażowe i popytowe:

Promowanie i wykorzystanie open source na rzecz suwerenności technologicznej

Komisja Europejska we współpracy z państwami członkowskimi podejmie działania w celu skalowania istniejących rozwiązań, m.in. poprzez rozbudowę katalogu *Open Internet Stack* jako unijnego punktu kompleksowej obsługi. Otwarte oprogramowanie stanie się domyślnym standardem dla ekosystemu Europejskiego Portfela Tożsamości Cyfrowej (EUID) oraz Europejskiego Portfela Biznesowego (EBW), a opieka nad nimi zostanie powierzona specjalnej Fundacji. Ukierunkowane inwestycje obejmą obszary o znaczeniu krytycznym: architekturę sprzętową (RISC-V), systemy operacyjne, stosy chmurowe, cyberbezpieczeństwo oraz otwarte modele AI wykorzystujące unijne superkomputery. Ponadto open source zostanie zintegrowany ze strategicznymi sektorami przemysłu (motoryzacja, lotnictwo, kolejnictwo, energia).

Wzmocnienie i promowanie ekosystemu open source

Aby przekształcić oddolne inicjatywy w stabilne biznesy, UE uruchomi dedykowane akceleratory biznesowe oferujące wsparcie prawne, licencyjne i marketingowe. W celu strukturyzacji zarządzania projektami, Komisja ułatwi tworzenie europejskich organizacji powierniczych (stewardów open source), opracowując tzw. *stewardship toolkit*. W zakresie bezpieczeństwa, we współpracy z EUAC (European Union Agency for Cybersecurity), opracowana zostanie lista zależności w oprogramowaniu, a nowo powołany Instrument Utrzymania Otwartego Oprogramowania (*Open Source Maintenance Instrument*) zapewni

[27] https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy

środki na techniczne utrzymanie kodu oraz awaryjne tworzenie bezpiecznych repozytoriów lustrzanych.

Promowanie otwartych i interoperacyjnych ekosystemów dla administracji publicznej

Sektor publiczny ma stać się głównym klientem napędzającym popyt poprzez wdrożenie zasady „pierwszeństwa open source" (*open source first principle*) w zakupach rządowych. Komisja wyda oficjalne wytyczne, jak projektować specyfikacje istotnych warunków zamówienia, by otwarte rozwiązania mogły uczciwie konkurować z zamkniętymi podmiotami własnościowymi. KE wdraża tę zasadę u siebie. Cyfrowe inwestycje publiczne będą opierać się na kryteriach otwartości i suwerenności na poziomie projektowym (*openness and sovereignty-by-design*). Działania te wspiera sieć biur OSPO (*Open Source Programme Office and EU Public Sector OSPO Network*).

Wzmocnienie standardów technologicznych i zasięg międzynarodowy

Działając w ramach podejścia *Team Europe*, UE będzie wspierać europejskich twórców w eksporcie ich rozwiązań (np. portfeli cyfrowych czy struktur internetowych) do krajów objętych procesem rozszerzenia oraz partnerów globalnych (wykorzystując programy *Global Gateway* i *Pact for the Mediterranean*). Z perspektywy wewnętrznej, planowana rewizja Unijnego Rozporządzenia Standaryzacyjnego wprowadzi mechanizmy trwałego włączenia społeczności open source w procesy tworzenia norm technicznych, co ułatwi m.in. implementację wymogów CRA (Cyber Resilience Act).

EWALUACJA STRATEGII

Wdrażanie strategii ma charakter wieloletni i będzie ściśle monitorowane w oparciu o ramy wskaźnikowe. Postępy będą corocznie omawiane z państwami członkowskimi w ramach Rady ds. Cyfrowej Dekady (*Digital Decade Board*), a co trzy lata Komisja przedłoży oficjalny raport Parlamentowi Europejskiemu i Radzie. Państwa członkowskie zostały wezwane do uwzględnienia celów strategii na poziomie krajowym poprzez grudniową (2026 r.) rewizję swoich Krajowych Strategicznych Map Drogowych Cyfrowej Dekady.

Strategic Roadmap on digitalization and AI in the energy sector[28]

WPROWADZENIE

Powołując się na raport Mario Draghiego, dokument wskazuje, że UE musi pilnie zainwestować w infrastrukturę danych i AI, aby utrzymać konkurencyjność przemysłu i obniżyć rachunki gospodarstw domowych. Kryzys jest potęgowany przez niestabilność cen paliw kopalnych wywołaną m.in. konfliktem na Bliskim Wschodzie.

Pełna integracja rozwiązań cyfrowych i elastyczności popytu do 2030 r. może przynieść konsumentom w UE do 71 mld EUR bezpośrednich oszczędności rocznie, a całemu systemowi korzyści rzędu 300 mld EUR. Wdrożenie rozwiązań AI w utrzymaniu elektrowni przyniesie globalnie 95 mld EUR oszczędności rocznie do 2035 r.

[28] https://energy.ec.europa.eu/publications/strategic-roadmap-digitalisation-and-ai-energy-sector_en

Centra danych konsumują obecnie ok. 2,5% prądu w UE. Do 2030 r. w gospodarkach rozwiniętych pochłoną one ponad 20% całego wzrostu zapotrzebowania na energię, tworząc poważną presję na zasoby wodne. UE musi zachować wyłączną kontrolę nad modelami AI i algorytmami w energetyce, konkurując w globalnym wyścigu z USA oraz Chinami.

Strategiczny plan działania opiera się na trzech filarach: Filar I dotyczy zrównoważonej integracji centrów danych z systemem energetycznym; Filar II określa środki służące wdrażaniu rozwiązań cyfrowych i AI w całym systemie energetycznym; natomiast Filar III dotyczy ram zarządzania danymi niezbędnych do umożliwienia inteligentnych usług energetycznych i stosowania AI na dużą skalę.

FILAR I – ENERGIA DLA AI (ZRÓWNOWAŻONA INTEGRACJA CENTRÓW DANYCH)

Pierwszy filar dokumentu koncentruje się na zrównoważonej integracji centrów danych z unijnym systemem energetycznym. Obiekty te są kluczowe dla cyfrowej suwerenności, a UE dąży do potrójnego zwiększenia ich wydajności w ciągu najbliższych 5-7 lat. Taki rozwój generuje jednak olbrzymie zapotrzebowanie na energię – oczekuje się, że zainstalowana moc centrów danych wzrośnie z około 12 GW w 2025 roku do około 28 GW w 2030 roku. Gwałtowny przyrost wniosków o przyłączenie do sieci, bez proaktywnego zarządzania, może zagrozić bezpieczeństwu dostaw, nasilić kongestię sieci i podbić ceny prądu.

W celu eliminacji barier Komisja kładzie nacisk na efektywne wykorzystanie sieci oraz wprowadzenie odpowiednich zachęt regulacyjnych i elastycznych umów przyłączeniowych dla centrów danych. Zapowiedziano również działania na rzecz przyspieszenia procedur wydawania pozwoleń, rezygnację z zasady „kto pierwszy, ten lepszy" na rzecz dojrzałości projektów oraz wykorzystanie unijnego portalu *Capacitypedia* do lokalizowania inwestycji.

Działanie Flagowe 1 – Trójstronne Umowy Modelowe (Model Tripartite Agreement): Publikacja w drugiej połowie 2026 r. wzorca umów łączących władze lokalne, operatorów centrów danych oraz podmioty energetyczne. Umowy te zlikwidują spekulacyjne blokowanie kolejek przyłączeniowych (zasada *use-it-or-lose-it*), zoptymalizują umowy PPA (Power Purchase Agreements) poprzez zapewnienie dodatkowej generacji czystej energii, dostarczanie rozwiązań w zakresie elastyczności centrów danych, wspieranie odzysku i wykorzystania ciepła odpadowego oraz poprawę efektywności energetycznej.

Działanie Flagowe 2 – Unijny system oceny i certyfikacji obejmujący efektywność energetyczną, efektywność gospodarki wodnej, wykorzystanie czystej energii, ponowne wykorzystanie ciepła odpadowego oraz elastyczność, a także uruchomienie procesu wprowadzania minimalnych unijnych standardów charakterystyki energetycznej. Pierwsze etykiety (labels) zostaną wydane w 2027 r., i w tym samym roku rozpocznie się proces definiowania minimalnych standardów wydajności dla nowych i starych obiektów.

FILAR II – CYFRYZACJA I AI DLA SYSTEMU ENERGETYCZNEGO

W miarę postępu elektryfikacji i dekarbonizacji, sieci elektroenergetyczne stają się kluczowym kręgosłupem zintegrowanego i odpornego systemu energetycznego. Aby sprostać

nowym wyzwaniom, infrastruktura ta musi stać się nie tylko silniejsza, ale również znacznie inteligentniejsza oraz odporniejsza na zmiany klimatyczne i zdarzenia ekstremalne. Cel ten ma zostać osiągnięty m.in. poprzez powszechne wykorzystanie danych geoprzestrzennych oraz zaawansowanych rozwiązań opartych na sztucznej inteligencji, które pozwolą zminimalizować ryzyka związane z klęskami żywiołowymi.

Inteligentne sieci zapewniają operatorom widoczność w czasie rzeczywistym, pełną interoperacyjność oraz kontrolę niezbędną do optymalizacji pracy całego systemu i efektywnego zwiększania udziału energii odnawialnej. Choć inwestycje w unowocześnianie europejskich sieci są kluczowe, ich rozwój wciąż napotyka na poważne bariery. Należą do nich przede wszystkim przestarzałe praktyki planistyczne i regulacyjne, które faworyzują tradycyjną, fizyczną rozbudowę infrastruktury zamiast wdrażania rozwiązań cyfrowych, a także niepewność rynkowa co do wydajności nowych technologii.

Ramy prawne Unii Europejskiej już teraz wspierają inwestycje w inteligentne sieci poprzez mechanizmy rynkowe oraz unijne fundusze badawcze, kładąc nacisk na promowanie rozwiązań alternatywnych wobec tradycyjnej rozbudowy infrastruktury. Istotnym elementem strategii jest wdrożenie przepisów dotyczących inteligentnych liczników (ang. smart metering), które stworzą warunki do bardziej efektywnego wykorzystania istniejących aktywów sieciowych za pomocą narzędzi cyfrowych.

W tym celu krajowe organy regulacyjne zostaną zobowiązane do ustanowienia specjalnych wskaźników wydajności dla operatorów systemów przesyłowych i dystrybucyjnych, co ułatwi m.in. wdrażanie technologii ulepszania sieci. Dodatkowo Komisja Europejska wspiera operatorów w rozwoju i masowym wdrażaniu technologii cyfrowych bliźniaków (ang. digital twins), dostarczając dedykowane narzędzia poprawiające ich skalowalność i interoperacyjność w codziennym zarządzaniu siecią. Ponieważ efektywne zarządzanie systemem zależy od dostępu do dokładnych i szczegółowych danych, kluczowym warunkiem pozostaje aktywne włączenie odbiorców końcowych, którzy dzięki systemom smart metering zyskają możliwość realnego udziału w programach elastyczności popytu i korzystania z umów z dynamiczną ceną energii.

Strategia wyraźnie podkreśla, że cyfryzacja pojedynczych podmiotów nie jest wystarczająca – pełen potencjał technologiczny zostanie uwolniony tylko wtedy, gdy rozwiązania AI zostaną wdrożone w całym łańcuchu wartości: od generacji ze źródeł odnawialnych, przez przemysł i budynki, aż po mobilność.

W kontekście globalnego wyścigu technologicznego, dla zachowania suwerenności UE kluczowe jest, aby nowe modele i algorytmy były rozwijane oraz zarządzane na terenie Europy przez unijne firmy i w oparciu o europejskie standardy oraz dane. Komisja Europejska planuje wspieranie rozwoju dedykowanych modeli bazowych AI, które po przeszkoleniu na różnorodnych zbiorach danych posłużą jako cyfrowy kręgosłup systemu, usprawniając prognozowanie, wykrywanie awarii czy zarządzanie ograniczeniami przesyłowymi. Narzędzia AI mają również zoptymalizować pracę elektrowni odnawialnych i jądrowych oraz wspomóc

planowanie renowacji budynków, zwłaszcza w uboższych energetycznie gospodarstwach domowych. W ramach unijnych programów badawczo-innowacyjnych szczególny nacisk zostanie położony na podejście otwarte (open source), a europejscy innowatorzy i startupy otrzymają ułatwiony dostęp do unijnej infrastruktury obliczeniowej oraz funduszy wzrostowych.

Działanie Flagowe 3 – Wskaźniki sieciowe i liczniki: Do połowy 2026 r. sfinalizowany zostanie katalog wskaźników inteligentnych sieci. W 2026 r. Komisja przedstawi projekt przepisów przyspieszających obowiązkową instalację inteligentnych liczników (*smart meters*) w państwach członkowskich, a w 2028 r. zostaną wydane rekomendacje dotyczące wskaźników wydajności sieci cyfrowych.

Działanie Flagowe 4 – Rozwój modeli AI w energetyce: W 2026 r. (30 mln EUR) i 2027 r. (20 mln EUR) ruszą dedykowane konkursy grantowe oraz wspólnota praktyków ds. AI w sieciach (Community of Practice). Testowe modele *proof-of-concept* powstaną w Q1 2027 r., a operacyjne do końca 2027 r. Równolegle w 2027 r. zaplanowano projekt, a w 2028 r. wdrożenie portali opartych na generatywnym AI, które zautomatyzują i przyspieszą urzędowe procedury wydawania pozwoleń na budowę OZE i sieci.

FILAR III – DANE DLA AI I SYSTEMU ENERGETYCZNEGO

Efektywna wymiana danych energetycznych oraz ich interoperacyjność są kluczowe dla rozwoju inteligentnych usług energetycznych i budowy solidnych modeli AI. Istniejące ramy prawne regulują wprawdzie wykorzystanie pierwotne danych (operacyjnych, takich jak fakturowanie, metryki czy zmiana dostawcy), jednak ich wdrożenie różni się w zależności od państwa członkowskiego. Stwarza to barierę dla rozwoju transgranicznych usług, zmuszając dostawców (np. inteligentnego ładowania aut) do ciągłego przebudowywania interfejsów i renegocjowania procedur dostępu na każdym rynku krajowym. Jeszcze mniej rozwinięte są ramy dotyczące wtórnego wykorzystania danych, czyli ich agregacji na potrzeby badań, analityki czy trenowania sztucznej inteligencji. Z powodu braku jasnych, sektorowych reguł i fragmentacji baz, operatorzy obawiają się dzielić szczegółowymi informacjami, co spowalnia rozwój AI przez konieczność pracy na danych syntetycznych lub ograniczonych.

Głównym wyzwaniem jest brak spójnego, unijnego podejścia do bezpiecznej, transgranicznej wymiany danych. Aby zapełnić tę lukę, Komisja Europejska koordynuje działania zmierzające do uproszczenia procedur zarówno dla pierwotnego, jak i wtórnego użytku, w ścisłej synergii z horyzontalnymi ramami cyfrowymi UE i Europejskimi Portfelami Tożsamości Cyfrowej. W obszarze wykorzystania pierwotnego celem jest ujednolicenie zasad i stworzenie wspólnych interfejsów dla stacji ładowania czy pomp ciepła, co pozwoli odblokować do 230 GW elastyczności systemu do 2030 roku. W zakresie użytku wtórnego nacisk zostanie położony na bezpieczne łączenie danych do szkolenia modeli AI, tworzenie piaskownic regulacyjnych oraz motywowanie operatorów sieciowych do współpracy, co docelowo pozwoli na stworzenie jednolitego i skalowalnego rynku inteligentnych usług energetycznych w UE.

Działanie Flagowe 5 – Unijne ramy wymiany danych: polega na stworzeniu jednolitych unijnych ram prawno-technicznych, które uproszczą transgraniczną wymianę danych energetycznych. Rozwiązanie to ma na celu wsparcie rozwoju inteligentnych usług energetycznych oraz ułatwienie trenowania zaawansowanych modeli sztucznej inteligencji. Wdrożenie inicjatywy zaplanowano dwuetapowo: etap przygotowawczy i ocena rozwiązań nastąpi w 2026 roku, natomiast implementacja ram prawnych ruszy od 2027 roku.

BEZPIECZEŃSTWO SEKTORA

Cyfryzacja infrastruktury krytycznej zwiększa wydajność, ale rodzi ryzyka cybernetyczne i hybrydowe. Powołana zostanie europejska grupa ds. transformacji bezpieczeństwa AI w energetyce, która zapewni nadzór ludzki i przejrzystość algorytmów. W latach 2020-2024 liczba cyberataków na podmioty energetyczne wzrosła trzykrotnie. Sektory wiatrowy i słoneczny są najbardziej narażone na sabotaż, manipulację produkcją i zdalne blackouty. W odpowiedzi KE ogranicza finansowanie projektów z falownikami od dostawców wysokiego ryzyka, a nowelizacja Aktu o Cyberbezpieczeństwie (Cybersecurity Act) umożliwi wprowadzenie całkowitego zakazu ich stosowania.

Skoordynowane działania UE mają kluczowe znaczenie dla globalnego zarządzania energią i cyfryzacją. Główne inicjatywy obejmują:

- **Od 2026 r.:** Współpraca z partnerami (np. w ramach G7) nad synergią energii i sztucznej inteligencji (AI).
- **Od 2027 r.:** Pierwsze pokazy transferu wiedzy technologicznej do krajów partnerskich (inicjatywa *AI for Public Good*).
- **Do 2028 r.:** Uruchomienie globalnej inicjatywy dotyczącej narzędzi cyfrowych i AI w transformacji energetycznej miast oraz walce z ubóstwem energetycznym.

Działanie Flagowe 6 — Bezpieczeństwo AI i urządzeń krytycznych: W 2026 r. przeprowadzona zostanie systemowa ocena ryzyka instalacji słonecznych w UE oraz nastąpi gruntowna rewizja ram bezpieczeństwa dostaw energii pod kątem IT.

WDRAŻANIE STRATEGICZNEGO PLANU DZIAŁANIA

Działanie Flagowe 7 – Monitoring i Inicjatywa „Better Energy Data”: Nastąpi wdrożenie stałej kontroli postępów do 2030 r. poprzez:

1. Coroczne Forum Cyfryzacji Energii (od 2026 r.).
2. Opracowanie wskaźników adopcji technologii w 2027 r.
3. Uruchomienie Obserwatorium Paliw (*Fuel Observatory*) w 2026 r.
4. Uruchomienie inicjatywy Lepszych Danych Energetycznych (*Better Energy Data*) w Q4 2026 r**.** w celu uzupełnienia luk informacyjnych.

Lista źródeł

Organizacje – krajowe i międzynarodowe

Komisja Europejska – Pakiet Suwerenności Cyfrowej

https://eur-lex.europa.eu/legal-content/EN/TXT/DOC/?uri=CELEX:52026PC0502

https://digital-strategy.ec.europa.eu/en/library/proposal-chips-act-20

https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy

https://energy.ec.europa.eu/publications/strategic-roadmap-digitalisation-and-ai-energy-sector_en

Komisja Europejska – Raport Cyfrowa Dekada

https://digital-strategy.ec.europa.eu/en/factpages/poland-2025-digital-decade-country-report?utm

https://digital-strategy.ec.europa.eu/en/library/state-digital-decade-2026-closing-structural-gaps-and-mobilising-investments-2030-and-beyond

Ministerstwo Cyfryzacji RP

https://samorzad.gov.pl/web/gov/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025?utm

https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-zmieniajacej-uchwale-w-sprawie-ustanowienia-programu-rzadowego-pod-nazwa-program-rozwoju-kompetencji-cyfrowych

PARP

https://www.parp.gov.pl/component/publications/publication/survey-report-global-entrepreneurship-monitor-poland-2025

Administracja USA

https://www.whitehouse.gov/wp-content/uploads/2026/04/NSTM-4.pdf

Raporty i analizy

World Economic Forum

https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

DigitalPoland

https://digitalpoland.org/publikacje/pobierz?id=3fd02f02-bed7-45cf-a29e-6908ac83f16e

OSW

https://www.osw.waw.pl/pl/publikacje/raport-osw/2025-12-17/smartfony-na-kolkach

Sektor prywatny

Anthropic

https://www.anthropic.com/glasswing

https://www.anthropic.com/news/securing-america-s-compute-advantage-anthropic-s-position-on-the-diffusion-rule?aff=47lw0&utm

Google DeepMind

https://storage.googleapis.com/deepmind-media/DeepMind.com/Blog/securing-the-future-of-ai-agents/gdm-ai-control-roadmap.pdf

Prasa

Rzeczpospolita

https://pro.rp.pl/raporty-ekonomiczne/art43099091-polskie-firmy-zyja-w-iluzji-cyberbezpieczenstwa?utm

https://cyfrowa.rp.pl/ai/art44659851-doktryna-wewnetrznego-wroga-dolina-krzemowa-przestaje-ufac-ai

https://www.rp.pl/biznes/art44749231-polska-uzyskala-dostep-do-poteznej-broni-ai

https://cyfrowa.rp.pl/ai/art44746621-usa-wycofaly-blokade-na-potezna-ai-anthropic-wraca-do-gry

Reuters

https://www.reuters.com/world/asia-pacific/china-restricts-overseas-travel-top-ai-talent-alibaba-deepseek-bloomberg-news-2026-05-26/?utm

https://www.reuters.com/world/china/china-prepares-295-billion-plan-fund-nationwide-ai-buildout-bloomberg-news-2026-06-09/?utm

https://www.reuters.com/technology/us-blocks-foreign-access-anthropics-most-advanced-ai-models-axios-reports-2026-06-13/?utm

Portale branżowe

https://gdpr.pl/ai-cyberbezpieczenstwo-i-odpornosc-cyfrowa-najwazniejsze-regulacje-ue-i-polski-czesc-i

https://crn.pl/aktualnosci/77-proc-polskich-firm-wydaje-na-cyberbezpieczenstwo-najwyzej-50-tys-zl-rocznie/?utm

PARP
Grupa PFR

Infolinia: 801 332 202

kontakt@parp.gov.pl

Obserwuj nas także na: