

Warszawa, dnia 12 czerwca 2024 r.

*Szanowni Państwo,*

w imieniu Związku Cyfrowa Polska, branżowej organizacji pracodawców zrzeszającej przedsiębiorstwa z sektora nowoczesnych technologii, pragnę przedstawić nasze stanowisko dotyczące kluczowych obszarów przyszłej polityki cyfrowej Unii Europejskiej oraz propozycji kierunków jej rozwoju. Dynamicznie zmieniający się krajobraz technologiczny wymaga podejścia kompleksowego, które obejmuje liczne aspekty życia społecznego i gospodarczego. Wierzymy, że nasze rekomendacje będą cennym wkładem w kształtowanie filarów polityki cyfrowej podczas polskiej prezydencji w Radzie UE oraz prac organów Unii Europejskiej w nadchodzącej kadencji.

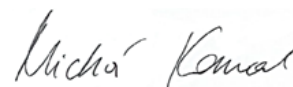
Nasze propozycje skupiają się na kilku kluczowych obszarach, w tym na:

- *sztucznej inteligencji,*
- *rozwijaniu infrastruktury i usług chmurowych,*
- *wzmacnianiu cyberbezpieczeństwa,*
- *identyfikacji elektronicznej i usługach zaufania,*
- *łączności gigabitowej,*
- *kompetencjach cyfrowych,*
- *finansowaniu polityki cyfrowej.*

Uważamy, że polityka cyfrowa Unii Europejskiej powinna być nie tylko nowoczesna i innowacyjna, ale również w pełni odpowiadająca na potrzeby obywateli i przedsiębiorstw w całej Europie. Stąd nasz apel o wzięcie pod uwagę poniższych wniosków i sugestii w procesie kształtowania polityki cyfrowej UE. Poniżej przedstawiamy szczegółowe rekomendacje, mając nadzieję, że przyczynią się one do stworzenia bezpiecznej, konkurencyjnej i innowacyjnej przestrzeni cyfrowej w Europie.

Z wyrazami szacunku,

**Michał Kanownik**



**Prezes Zarządu**

**Związek Cyfrowa Polska**



## **Sztuczna inteligencja (AI)**

Wdrażanie sztucznej inteligencji jest dzisiaj podstawą do pobudzenia wzrostu gospodarczego poprzez zwiększenie produktywności, która znajduje się w fazie spowolnienia lub stagnacji w Europie. Wyższa produktywność, generowanie większej produkcji przy takim samym nakładzie pracy, pozwala gospodarkom rozwijać się bez wyczerpywania ograniczonych zasobów. Wzrost produktywności był również historycznie jednym z najlepszych sposobów na poprawę dochodów i warunków życia pracowników. Dlatego wdrażanie sztucznej inteligencji przez firmy i tempo tego procesu, wpłynie w przyszłości na różnice w dochodach między krajami. Apelujemy zatem o uwzględnienie poniższych rekomendacji w zakresie wspierania procesu wdrażania sztucznej inteligencji i kształtowania kierunków polityki cyfrowej UE w jej nowym cyklu instytucjonalnym (2024-2029) w czasie prezydencji Polski w Radzie UE w I połowie 2025 roku.

Rządy, które chcą przyspieszyć tempo wdrażania sztucznej inteligencji, mogą podjąć wiele działań, aby zachęcić do korzystania z tej technologii i przygotować swoją siłę roboczą, przedsiębiorstwa i sektor publiczny do „gotowości na sztuczną inteligencję”. Rządy mogą także dawać impuls rynkowy sektorowi prywatnemu, a jednocześnie wykorzystywać swoją siłę nabywczą do pobudzenia popytu na towary i usługi związane ze sztuczną inteligencją. Inwestowanie w szkolenia i podnoszenie kwalifikacji pracowników oraz w krajowe chmury badawcze może pomóc w zapewnieniu odpowiedniej podaży talentów AI i mocy obliczeniowej, aby wykorzystać możliwości, które zostaną stworzone przez AI w nadchodzących latach.

Jak wykazały badania, podejście krajów-liderów AI do sztucznej inteligencji ma kilka cech wspólnych:

- przewidują znaczące inwestycje w fundamenty umożliwiające udany ekosystem sztucznej inteligencji (w tym edukację, podnoszenie kwalifikacji siły roboczej i dostęp do obliczeń);
- obejmują strategiczne wysiłki na rzecz przyspieszenia przyjęcia AI w priorytetowych branżach w sektorze publicznym i prywatnym;
- przewidują, że uczelnie wyższe będą działać jako motory innowacji, kreując lokalnie możliwości rozwoju i współpracując z przemysłem i rządem.

Zalecamy, aby w ramach polityki cyfrowej, wprowadzać implementację przez rządy 10-etapowego pakietu działań, w połączeniu z ukierunkowanym podejściem do regulacji.



Działania po stronie „podażowej”:

1. Inwestowanie w talenty, aby zapewnić, że podaż zaspokoi popyt. Około 42% firm wymienia dostęp do talentów jako główną barierę we wdrażaniu sztucznej inteligencji.
2. Promowanie większego udziału niedostatecznie reprezentowanych grup w ekosystemie sztucznej inteligencji.
3. Zachęcanie do podnoszenia kwalifikacji w zakresie sztucznej inteligencji zarówno specjalistów IT, jak i pracowników niezwiązanych z ICT w sektorze prywatnym i publicznym.
4. Ustanowienie krajowych chmur badawczych jako zasobu wspierającego badania akademickie, lokalne startupy i przypadki użycia w sektorze publicznym.
5. Regulacje powinny być ukierunkowane i proporcjonalne.

Działania po stronie „popytowej”:

6. Wspieranie MŚP w zarządzaniu wdrażaniem sztucznej inteligencji, umożliwiające skalowanie działalności.
7. Inwestowanie w sztuczną inteligencję w celu poprawy usług publicznych.
8. Wspieranie innowacyjnego podejścia do badań i rozwoju w zakresie sztucznej inteligencji finansowanych ze środków publicznych.
9. Gromadzenie, opracowywanie i prowadzenie regularnych badań dotyczących krajowych trendów w zakresie wdrażania sztucznej inteligencji i wykorzystanie informacji w planowaniu wdrażania AI.
10. Wskazanie priorytetowych sektorów o strategicznym znaczeniu, bowiem adopcja AI jest zwykle nierównomierna w różnych gałęziach przemysłu.



## Chmura obliczeniowa

Jednym z elementów nowej polityki cyfrowej w Unii Europejskiej ma być infrastruktura i usługi chmurowe. W związku z powyższym opublikowany został projekt białej księgi: „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej?”. Rozwiązania projektowane w obecnym brzmieniu białej księgi niosą za sobą szereg zagrożeń. Zignorowanie ich może wiązać się z licznymi negatywnymi konsekwencjami zarówno dla branży, jak i dla samych konsumentów. Apelujemy zatem o uwzględnienie poniższych wniosków w procesie kształtowania kierunków polityki cyfrowej UE w jej nowym cyklu instytucjonalnym (2024-2029) w czasie z Przewodnictwa Polski w Radzie UE w I połowie 2025 r.

Najważniejsze wnioski dotyczące rozważanych regulacji:

- rynek związany z wykorzystaniem chmury w sektorze telekomunikacyjnym nie wymaga dodatkowych regulacji ponad obowiązujące przepisy UE;
- nie ma żadnej konwergencji między usługami w chmurze a usługami telekomunikacyjnymi. Działania regulacyjne powinny utrzymać istniejące od dawna rozróżnienie między dostawcami usług w chmurze a operatorami telekomunikacyjnymi;
- nałożenie znaczących obciążeń regulacyjnych może ograniczyć innowacyjność na rynku chmury;
- powrót do koncepcji opłat sieciowych może się wiązać dla konsumentów z gorszą jakością usług i wzrostem kosztów;
- rozszerzenie zakresu usługi powszechnej w celu subsydiowania infrastruktury światłowodowej w obszarach odległych oraz udział w tym finansowaniu usług łączności interpersonalnej niewykorzystujących numerów miałyby szkodliwe skutki dla konsumentów i przedsiębiorstw.

W białej księdze „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej?” przedstawiony został pomysł objęcia dostawców usług w chmurze i CDN mechanizmami rozstrzygania sporów dotyczących połączeń międzysieciowych. Zwracamy uwagę, że jest to koncepcja, która w rzeczywistości jest powrotem do propozycji wprowadzenia opłat sieciowych. Pomysł ten został odrzucony w ubiegłym roku przez państwa członkowskie z uwagi na zdecydowany opór ze strony zarówno państw członkowskich, jak i organizacji pozarządowych, czy też przemysłu europejskiego. Okazało się jednak, że Komisja Europejska chciałaby powrócić do tego pomysłu, tym razem pod postacią mechanizmu rozstrzygania sporów.



Konsekwencje wprowadzenia dodatkowych opłat internetowych odczuliby zarówno przedsiębiorcy, jak i konsumenci. Obecnie chmurę stosuje się powszechnie do przeprowadzania transformacji cyfrowej. Wśród różnych usług w chmurze, sieci dystrybucji treści umożliwiają europejskim firmom, które tworzą treści (wideo, gry itp.), przechowywanie treści w pamięci podręcznej blisko użytkowników końcowych, zmniejszając w ten sposób opóźnienia dla konsumentów, ilość ruchu, który przechodzi przez sieci operatorów telekomunikacyjnych, zużycie energii oraz koszty tranzytu operatorów telekomunikacyjnych.

Powiększenie zakresu mechanizmu sporów o połączenia międzysieciowe jako mechanizmu wdrażania opłat sieciowych miałyby wpływ na wszystkie te europejskie organizacje, które korzystają z usług klientów chmurowych i CDN w celu dostarczania treści użytkownikom końcowym. Zostaną one obciążone dodatkowymi kosztami. Co więcej, opłaty nakładane na połączenia międzysieciowe, które nie są oparte na negocjacjach i wartości rynkowej, sprawiają, że dostawcy CDN będą preferować alternatywne, tańsze ścieżki (tranzyt) zamiast bezpośredniego połączenia, co doprowadzi do spadku wydajności i dodatkowych kosztów operacyjnych zarówno dla dostawców usług CDN, jak i dostawców usług internetowych.

Ostatecznie będzie to miało wpływ na konsumentów, jako że wzrosną koszty i pogorszy się doświadczenie użytkownika (w szczególności poprzez zwiększenie opóźnień). Tak właśnie stało się w Korei Południowej, gdzie w 2016 r. wprowadzono regulację połączeń międzysieciowych. Doprowadziło to do wzrostu cen połączeń międzysieciowych. Niektóre firmy zdecydowały się przenieść swoje serwery treści poza Koreę (zwiększając opóźnienia dla konsumentów), inne zdecydowały się nie oferować już usług w Korei.

### **Cyberbezpieczeństwo**

Zagrożenia i incydenty cyberbezpieczeństwa wzrosły dramatycznie w ostatnich latach, a nowi aktorzy starają się uzyskiwać dostęp do systemów, wykraść wrażliwe dane i naruszać bezpieczeństwo infrastruktury krytycznej. Te zmieniające się wyzwania związane z cyberbezpieczeństwem wymagają skoordynowanej reakcji, która połączy sektor publiczny i prywatny z krajów *like-minded*. Zagrożenia cybernetyczne nie są ograniczone do jednego regionu, ale mają niemal uniwersalne znaczenie ze względu na rozprzestrzenianie się technologii na całym świecie.



W ciągu ostatnich 5 lat UE uruchomiła szeroką gamę inicjatyw na rzecz stworzenia bezpieczniejszej i bardziej odpornej Europy. Postulujemy aby polska prezydencja przy kształtowaniu szczegółowej agendy cyfrowej i polityki cyberbezpieczeństwa na poziomie UE, wzięła pod uwagę poniższe zalecenia z korzyścią dla europejskich obywateli, przedsiębiorstw i administracji publicznej.

Niedawno przyjęte europejskie prawodawstwo dotyczące cyberbezpieczeństwa jest obszerne pod względem zakresu i szczegółowości. Zarówno przedsiębiorstwa, jak i rządy będą musiały skoncentrować swoje wysiłki na wdrażaniu i nadzorowaniu nowych przepisów. Wszelkie nowe wnioski ustawodawcze powinny ograniczać się jedynie do inicjatyw, które rozwiązują rzeczywiste luki regulacyjne lub oferują uproszczenia. Co do zasady nowe wymogi powinny być oparte na dowodach, oparte na ryzyku i proporcjonalne, neutralne technologicznie, z naciskiem na przewidywalne wyniki. Dzięki temu nowe przepisy zwiększą bezpieczeństwo i odporność oraz zapobiegą tworzeniu niepotrzebnych barier handlowych lub obciążeń związanych z przestrzeganiem przepisów dla przedsiębiorstw.

Priorytetem powinno być ulepszenie mechanizmów obejmujących zakresem sektor prywatny w celu wspierania wdrażania wymogów prawnych. Pomimo szeregu inicjatyw w zakresie cyberbezpieczeństwa, nie ma wspólnej grupy interesariuszy z różnych obszarów gospodarki, która zajmowałaby się horyzontalnym zastosowaniem ram bezpieczeństwa cybernetycznego. Utworzenie takiego forum może pomóc ENISA i Komisji Europejskiej w tworzeniu wspólnych wytycznych oraz pomóc uniknąć fragmentacji jednolitego rynku i wesprzeć wspólne ramy zarządzania cybernetycznego. Przegląd Aktu o Cyberbezpieczeństwie mógłby stanowić okazję do przeprowadzenia tej niezbędnej reformy.

Istnieje potrzeba głębszego inwestowania we współpracę z krajami o podobnych poglądach (like-minded) w celu wspierania bezpieczeństwa i odporności. Przyjmując zharmonizowane podejście polityczne i promując przyjęcie wspólnych standardów wśród swoich partnerów, UE wzmacnia swoją odporność, jednocześnie promując globalne i otwarte podejście, które przynosi korzyści europejskim przedsiębiorstwom. Rozszerzenie istniejących kanałów dialogu lub budowanie szerszych forów wielostronnych może pomóc UE zwiększyć sieć partnerów podobnie nastawionych do walki z zagrożeniami cybernetycznymi.

Zwiększenie współpracy z podmiotami ze świata biznesu w celu zidentyfikowania i rozwiązania potencjalnych skutków proponowanych systemów certyfikacji. Takie podejście pomoże stworzyć ramy certyfikacji cyberbezpieczeństwa dostosowane do potrzeb społeczności biznesowej, realizując wspólne ambicje zwiększonego bezpieczeństwa produktów, usług i systemów cyfrowych.



Zapewnienie, by systemy certyfikacji cyberbezpieczeństwa i polityki bezpieczeństwa cybernetycznego były inkluzywne i niedyskryminacyjne, poszerzając zakres wyboru technologii w całej Europie. Pomoże to europejskim przedsiębiorstwom, w tym MŚP i start-upom, uzyskać dostęp do technologii potrzebnych do skalowania i rozwoju. Będzie również wspierać administracją publiczną, która musi szybko zwiększyć swoje możliwości w zakresie cyberbezpieczeństwa w miarę ewolucji zagrożeń.

Zlikwidowanie istniejącej luki w umiejętnościach poprzez włączenie kształcenia w zakresie cyberbezpieczeństwa do systemów edukacji, inicjatyw podnoszenia kwalifikacji oraz współpracy publiczno-prywatnej. Zapewni to przedsiębiorstwom i osobom fizycznym narzędzia potrzebne do rozwoju w cyfrowym świecie, wspierając wzrost i odporność europejskiej gospodarki cyfrowej.

### **Identyfikacja elektroniczna i usługi zaufania**

Nowelizacja Rozporządzenia eIDAS 2 ma dostarczyć rozwiązania umożliwiające jednolitą identyfikację elektroniczną oraz powszechną dostępność kwalifikowanych podpisów elektronicznych. Celem jest zwiększenie bezpieczeństwa i efektywności transakcji online. W tym kontekście, jednym z cyfrowych priorytetów powinna być budowa Europejskiego Portfela Tożsamości Cyfrowej. Ten krok ma na celu zwiększenie synergii między rynkiem publicznym, a prywatnym w całej Unii Europejskiej.

Europejski Portfel Cyfrowej Tożsamości ma zapewnić jednolity, wysoki poziom wiarygodności i bezpieczeństwa w całej Unii. Użytkownicy będą mogli bezpiecznie przechowywać i udostępniać swoje dane identyfikacyjne oraz elektroniczne poświadczenia atrybutów, co ułatwi korzystanie z różnorodnych usług online. Portfel ten będzie obowiązkowo akceptowany w szerokim zakresie usług, co stanowi znaczący krok w kierunku cyfryzacji i ujednoczenia usług w całej Unii.

Nowelizacja eIDAS 2 ma ogromne znaczenie dla darmowych podpisów kwalifikowanych do zastosowań "nieprofesjonalnych", które będą połączone z Europejskim Portfelem Tożsamości Cyfrowej. To zagadnienie ma ogromny potencjał w zakresie przekształcenia cyfrowego krajobrazu w Polsce i Europie. Należy zatem zapewnić trwałość oraz ciągłość konkurencyjności tego rynku. W naszej ocenie konieczna jest szeroka współpraca administracji publicznej z rynkiem komercyjnym w tym zakresie, również w kontekście aktów implementacyjnych. Administracja publiczna powinna skupić się na budowie portfela i udostępnieniu identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa, podczas gdy rynek prywatny może być naturalnym partnerem w budowaniu ekosystemu usług zaufania.



Cyfrowy portfel wzmocni bezpieczeństwo obywateli, którzy coraz częściej korzystają z usług mobilnych lub cyfrowych. Aspekty związane z certyfikacją urządzeń i rozwiązań zaczną odgrywać fundamentalną rolę w rozwoju cyfrowego biznesu. Ze względu na obecną sytuację geopolityczną oraz rosnącą z roku na rok falę zagrożeń cybernetycznych, jednym z priorytetowych działań powinno być wsparcie rozwoju usług cyfrowych wspomagających cyfrową transformację procesów biznesowych, w tym nowy wymiar usług opartych na rozwiązaniach mobilnych.

### **Łączność gigabitowa**

Cyfrowa transformacja Unii Europejskiej stale przyspiesza m. in. dzięki Programowi Cyfrowej Dekady. Jednym z jego filarów jest infrastruktura cyfrowa, która ma zapewnić pełne pokrycie populacji sieciami komórkowymi nowej generacji oraz siecią gigabitową.

Komisja Europejska określiła kluczowe wskaźniki efektywności służące do pomiaru postępów w realizacji celów cyfrowych. W ocenie Komisji jedynymi technologiami, które obecnie mogą zapewnić łączność gigabitową, są światłowód oraz sieć kablowa w standardzie DOCSIS 3.1. Niestety, tak sformułowane założenia nie są w stanie sprostać rzeczywistym potrzebom europejskich konsumentów, szczególnie na obszarach wiejskich i oddalonych oraz są nieracjonalne pod kątem finansowym.

Apelujemy zatem o uwzględnienie również satelitarnej łączności szerokopasmowej LEO (świadczonymi na niskiej orbicie) w planach dotyczących zaspokojenia potrzeb użytkowników końcowych w zakresie łączności w ramach Cyfrowej Dekady podczas przewodnictwa Polski w Radzie UE

Satelitarne łącza szerokopasmowe LEO już dziś są w stanie zapewnić znacznie wyższą jakość usług niż ta wymagana przez użytkowników końcowych (prędkość pobierania 100 Mb/s i opóźnienia poniżej 100 ms) w najtrudniej dostępnych obszarach UE. Z tego powodu błędem jest pominięcie tej technologii w planach Unii Europejskiej dotyczących infrastruktury cyfrowej. Zmiany w tym zakresie powinny znaleźć się wśród priorytetów w zakresie cyfryzacji.





Obecnie zwykle przyjmuje się, że prędkość pobierania 100 Mb/s jest wystarczająca dla 2-4 jednoczesnych użytkowników strumieniujących wideo 4K, grających w gry, pracujących z domu i korzystających z domowych urządzeń zabezpieczających. Większe przepustowości są wymagane tylko w wyjątkowych przypadkach z większą liczbą jednoczesnych użytkowników i gdy muszą oni uzyskać dostęp do aplikacji o dużej przepustowości (takich jak prowadzenie domowego biura, korzystanie z kreatywnych aplikacji / oprogramowania lub korzystanie z inteligentnych urządzeń domowych). Ustalenie to jest zgodne z raportem Ofcom z 2021 r., sugerującym, że tylko bardzo zaawansowane formy AR/VR będą wymagały większej przepustowości w przyszłości.

Ponadto, alternatywna łączność LEO stanowi dodatkowy filar podnoszenia cyberbezpieczeństwa i odporności. Pokazał to dobitnie przykład wojny w Ukrainie, gdzie rozwiązania LEO umożliwiły wsparcie łączności, niezależnie od naziemnej infrastruktury, jaka była dostępna na danym obszarze oraz od stopnia jej uszkodzenia.

Łącząc satelitarne sieci szerokopasmowe i tradycyjne sieci komórkowe, stacjonarne sieci bezprzewodowe i światłowodowe można zapewnić dostęp do Internetu większej liczbie użytkowników, nawet w regionach, które zawsze były odcięte od tego typu usług przez swoje położenie. Z kolei w miejscach, w których łączność istnieje, ale jest niewystarczająca, może pozwolić na zapewnienie bardziej niezawodnego i spójnego łącza, wspierając istniejącą już infrastrukturę.

Dlatego postulujemy uznanie zdolności satelitarnej łączności szerokopasmowej LEO do zaspokojenia potrzeb użytkowników końcowych w zakresie łączności w ramach Cyfrowej Dekady i promowanie takich rozwiązań w planach działania państw członkowskich.

### **Kompetencje cyfrowe**

Umiejętności cyfrowe mają zasadnicze znaczenie we współczesnym społeczeństwie i są kluczowe dla pełnego udziału w nowoczesnym życiu społecznym, gospodarczym i kulturalnym. W erze cyfrowej transformacji, te umiejętności wykraczają poza podstawowe korzystanie z komputerów i Internetu, obejmując także zdolności do krytycznego myślenia, rozwiązywania problemów oraz zapewniania bezpieczeństwa w sieci.



W ramach priorytetów polskiej prezydencji w Radzie UE, szczególną uwagę należy poświęcić rozwijaniu i doskonaleniu kompetencji cyfrowych obywateli. Obejmuje to wprowadzenie edukacji cyfrowej od najmłodszych lat, wsparcie dla nauczycieli i edukatorów, a także szkolenia dla pracowników różnych sektorów gospodarki. Wzmacnianie tych umiejętności jest niezbędne dla konkurencyjności europejskiego rynku pracy oraz dla zwiększenia innowacyjności i adaptacyjności firm wobec dynamicznych zmian technologicznych.

W obliczu rosnących zagrożeń cybernetycznych, edukacja w zakresie bezpieczeństwa cyfrowego nabiera szczególnego znaczenia. Obywatele powinni być świadomi ryzyk związanych z cyberprzestępczością i znać podstawowe zasady tzw. cyberhigieny. Wzmacnianie umiejętności cyfrowych w zakresie cyberbezpieczeństwa przyczyni się do tworzenia bezpieczniejszego środowiska cyfrowego.

Rozwój umiejętności cyfrowych to także inwestycja w przyszłość, przynosząca korzyści zarówno gospodarce, jak i całemu społeczeństwu. Polska prezydencja w Radzie UE powinna zatem aktywnie promować inicjatywy wspierające edukację cyfrową oraz dostęp do nowoczesnych technologii.

### **Infrastruktura cyfrowa**

Apelujemy o zmianę polityki dotyczącej sposobu finansowania infrastruktury mającej na celu zapewnienie łączności gigabitowej. W miejscach, w których usługi łączności satelitarnej na niskich orbitach (LEO) i 5G FWA mogą zaspokoić potrzeby użytkowników i zostać wdrożone taniej na warunkach rynkowych, powinno się rozważyć ograniczenie subsydiowania wyłącznie infrastruktury światłowodowej na rzecz rozwiązań tańszych, a jednocześnie bardziej praktycznych.

Pełne pokrycie gospodarstw domowych w Unii stałym i szybkim łączem szerokopasmowym wymaga zastosowania technologii uzupełniających, takich jak szybkie łącza szerokopasmowe LEO i 5G FWA. Wykorzystanie systemów szerokopasmowych LEO może rozszerzyć zasięg łączności oraz pozwolić rządowi UE na zaoszczędzenie miliardów na dotacjach światłowodowych finansowanych przez podatników. Satelitarne łącza szerokopasmowe LEO będą w stanie zapewnić znacznie wyższą jakość usług niż ta wymagana przez użytkowników końcowych (prędkość pobierania 100 Mb/s i opóźnienia poniżej 100 ms) w najtrudniej dostępnych obszarach UE.



Do 2030 r. planowane jest pokrycie gospodarstw domowych sieciami gigabitowymi na poziomie 91%, co i tak kosztować będzie ok. 68 mld euro w kapitale prywatnym i 29 mld euro w dotacjach. Po 2030 r. poziom 99% zasięgu wiązać się będzie z kosztem w postaci ok. 19 mld euro w kapitale prywatnym i 19 mld euro w dotacjach. Jak zatem widać, dotowanie sieci światłowodowych w miejscach oddalonych lub trudno dostępnych nie znajduje uzasadnienia. Takie działanie zaburza przy tym konkurencję z technologiami, które mogą zaspokoić potrzeby użytkowników końcowych w zakresie łączności w bardziej opłacalny sposób.

WIK-Consult sugeruje, że obszary, w których wdrażanie światłowodów nie będzie opłacalne (około 16% gospodarstw domowych w UE), wymagałyby średniej dotacji w wysokości 1200 euro na gospodarstwo domowe. Szacunki te mogą być jednak znacznie wyższe w przypadku najtrudniej dostępnych gospodarstw domowych. Sugeruje to, że subsydiowanie wdrożeń światłowodów, szczególnie w obszarach, w których komercyjnie oferowane satelitarne łącza szerokopasmowe LEO będą w stanie zaspokoić potrzeby użytkowników końcowych w bardziej opłacalny sposób, zakłóci konkurencję i spowoduje nieefektywne wykorzystanie zasobów państwowych. W dłuższej perspektywie zakłóci to również zachęty inwestycyjne, zmniejszając zachęty dla operatorów satelitarnych do inwestowania w ulepszanie swoich usług w czasie, aby konkurować ze światłowodami.

Konieczne jest stosowanie rozwiązań łączących satelitarne sieci szerokopasmowe i tradycyjne sieci komórkowe, stacjonarne sieci bezprzewodowe i światłowodowe. Pozwoli to na zapewnienie powszechniejszego dostępu do Internetu, a jednocześnie jest to rozwiązanie tańsze i szybsze. Nie wymaga ono bowiem długotrwałej budowy drogiej infrastruktury, a także jest mniej problematyczne w bieżącym utrzymaniu w terenach trudniej dostępnych.

Jednocześnie należy zapewnić, aby publiczne programy finansowania odbioru (takie jak bony socjalne lub bony na łączność) były neutralne technologicznie i nie faworyzowały żadnego konkretnego operatora satelitarnego, zgodnie z zasadami pomocy państwa.

### **Finansowanie polityki cyfrowej**

W Białej Księdze „Jak sprostać potrzebom Europy w zakresie infrastruktury cyfrowej?” Komisja Europejska opowiada się za rozszerzeniem zakresu usługi powszechnej o subsydiowanie infrastruktury światłowodowej na obszarach oddalonych i wiejskich, a także o objęcie usług komunikacji interpersonalnej niewykorzystujących numerów obowiązkiem dopłat do takich subsydiów. Jest to propozycja która będzie miała negatywne skutki dla konsumentów i firm. Apelujemy zatem o podjęcie działań na rzecz wstrzymania zmian zmierzających w tym kierunku.



Powyżej opisane rozwiązanie byłoby sprzeczne z postanowieniami Europejskiego Kodeksu Łączności Elektronicznej. Kodeks dopuszcza jedynie subsydiowanie przez USO „odpowiedniego dostępu szerokopasmowego”, który państwa członkowskie określiły jako dostęp do Internetu o przepustowości 30 Mb/s. Ponadto wskazujemy, że propozycja Komisji Europejskiej nie wynika z potrzeb użytkowników końcowych. Jedynie 14% konsumentów w UE korzysta z usługi 1 Gb/s, a średnia prędkość pobierania w UE wynosi obecnie tylko około 100 Mb/s. [Raport](#) przygotowany przez Arthura D. Little’a pokazuje, że w praktyce przepustowości poniżej 100 Mb/s są całkowicie wystarczające do zaspokojenia wszystkich wymogów użytkowników.

Dlatego właśnie konieczne jest zaniechanie subsydiowania rozwiązań nieadekwatnych do okoliczności. Państwa członkowskie powinny obrać podejście neutralne technologicznie i polegać na innych technologiach, takich jak szerokopasmowa łączność satelitarna na niskiej orbicie okołoziemskiej (LEO) i stacjonarny dostęp bezprzewodowy 5G.

Warto też nadmienić, że wpłaty od podmiotów cyfrowych na subsydiowanie infrastruktury światłowodowej na obszarach oddalonych i wiejskich, gdzie dostępne będą usługi szerokopasmowe LEO i 5G FWA, przyniosłyby bardzo ograniczone korzyści użytkownikom końcowym. Wręcz przeciwnie, zwiększyłyby koszty podmiotów cyfrowych dokonujących wpłaty na rzecz obowiązku świadczenia usługi powszechnej. Takie działanie miałyby negatywny wpływ na te firmy, a ostatecznie na użytkowników końcowych. Ponadto subsydiowanie światłowodów tam, gdzie inne technologie mogą zaspokoić potrzeby użytkowników końcowych w zakresie łączności, zakłóciłoby konkurencję i mogłoby być sprzeczne z zasadami pomocy publicznej.

Co więcej, badania ekonomiczne pokazują, że to treści napędzają popyt konsumentów na szybkie łącza szerokopasmowe. Według [raportu](#) Deloitte przygotowanego na zlecenie Amazon, wartość dostępu do treści przypisywana przez europejskich użytkowników Internetu jest od 2 do 5 razy wyższa niż koszty ich ruchu w sieciach telekomunikacyjnych. Dlatego dostawcy treści już teraz przyczyniają się do wzrostu wartości sieci telekomunikacyjnych, a dalsze opłaty w formie obowiązku świadczenia usługi powszechnej zwiększyłyby koszty dostawców treści i ostatecznie zaszkodziłyby popytowi na szybkie łącza szerokopasmowe.