Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów »Bezpieczne wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi«"

[COM(2020) 50 final]

(2020/C 429/37)

Sprawozdawca: **Alberto MAZZOLA**

Współsprawozdawca: **Dumitru FORNEA**

Wniosek o konsultację	Komisja Europejska, 9.3.2020
Podstawa prawna	Art. 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego
Data przyjęcia przez sekcję	3.9.2020
Data przyjęcia na sesji plenarnej	16.9.2020
Sesja plenarna nr	554
Wynik głosowania (za/przeciw/wstrzymało się)	217/0/2

1. **Wnioski i zalecenia**

1.1. EKES z zadowoleniem przyjmuje inicjatywę państw członkowskich i Komisji Europejskiej (KE) na rzecz weryfikacji wdrażania przez państwa członkowskie zestawu środków zalecanych we wnioskach dotyczących pakietu kluczowych strategicznych i technicznych środków bezpieczeństwa w zakresie wdrażania ekosystemu 5G.

1.2. EKES uważa, że z uwagi na coraz większą złożoność i różnorodność zastosowań 5G (KE ustaliła następujące cele dotyczące łączności na 2025 r.: szkoły, wyższe uczelnie, ośrodki badawcze, szpitale, główni dostawcy usług publicznych i przedsiębiorstwa prowadzące intensywną działalność w internecie powinny mieć dostęp do prędkości pobierania/wysyłania danych wynoszącej 1 GB danych na sekundę; miejskie i wiejskie gospodarstwa domowe powinny mieć dostęp do sieci połączeń o prędkości pobierania danych wynoszącej co najmniej 100 MB na sekundę; obszary miejskie, główne drogi i linie kolejowe powinny mieć nieprzerwany zasięg 5G), takie badanie ekosystemu 5G oraz działania w ramach kompetencji KE w celu zapewnienia cyberbezpieczeństwa sieci 5G i zdywersyfikowanego łańcucha wartości 5G, normalizacja techniczna i certyfikacja, bezpośrednie inwestycje zagraniczne, ochrona handlu i konkurencja, zobowiązania z tytułu świadczenia usług publicznych, zamówienia publiczne i dyplomacja cyfrowa powinny obejmować bezpieczeństwo geopolityczne, infrastrukturę, bezpieczeństwo danych oraz bezpieczeństwo sanitarne, w tym zgodnie z art. 168 ust. 1 TFUE.

1.3. Zdaniem EKES-u ważne jest, aby europejski ekosystem 5G zapewniał integralność, poufność, odpowiedzialność za zarządzanie i odpowiedzialność operacyjną, bezpieczeństwo, zamienność, interoperacyjność sprzętu i oprogramowania, wspólne standardy techniczne, ciągłość usług, niezawodność przepływu i ochronę danych, zasięg na wszystkich obszarach, w tym na obszarach słabo zaludnionych, jasność komunikacji z użytkownikiem działającym na rynku cyfrowym, dynamiczne stosowanie się do wytycznych Międzynarodowej Komisji ds. Ochrony Przed Promieniowaniem Niejonizującym (ICNIRP) w zakresie ochrony zdrowia ludności przy jednoczesnym jak największym ograniczeniu promieniowania. ICNIRP zaktualizował odpowiednio część wytycznych z 1998 r. o polach elektromagnetycznych i częstotliwościach radiowych. Dokument ten przedstawia zmienione wytyczne, które zapewniają ochronę ludzi przed narażeniem na pola elektromagnetyczne o częstotliwości od 100 kHz do 300 GHz. Health Phys. 118(5):483–524; 2020, marzec 2020 r. ICNIRP (2020 r.) wprowadził szereg zmian w celu zapewnienia, aby nowe technologie, takie jak 5G, nie były szkodliwe, niezależnie od związanych z nimi oczekiwań.

1.4. EKES wzywa KE do ścisłego monitorowania postępów we wdrażaniu i faktycznym wykorzystywaniu technologii 5G oraz wzywa państwa członkowskie do dalszego przyspieszenia tego procesu i zapewnienia jego odpowiedzialnej realizacji, z uwzględnieniem wszystkich aspektów bezpieczeństwa i ochrony, w tym aspektów dotyczących wpływu technologii 5G na zdrowie publiczne i żywe ekosystemy, wpływu na sytuację społeczno-gospodarczą i konkurencję, wpływu na kształcenie i szkolenia oraz gwarancji poszanowania praw podstawowych.

1.5. EKES apeluje, by UE stała się światowym liderem w technologii mobilnej kolejnej generacji 5G wyposażonej w bezpieczną infrastrukturę cyfrową jako solidny element nowej nowoczesnej europejskiej strategii przemysłowej poprzez radykalne przesunięcie w kierunku łączności mobilnej, z ogromnym potencjałem dynamicznym w zakresie zwiększenia wydajności i pobudzenia gospodarki i usług dla obywateli.

1.6. W szczególności EKES uważa, że zasadnicze znaczenie ma zapewnienie oceny profilu ryzyka dostawców oraz stosowanie odpowiednich ograniczeń w odniesieniu do dostawców uznawanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń w celu skutecznego określenia zobowiązań i ograniczenia ryzyka związanego z aktywami kluczowymi i wrażliwymi określonymi w unijnej skoordynowanej ocenie ryzyka.

1.7. EKES uważa za niezbędne, by Europa przyjęła średnioterminową wizję autonomii i samowystarczalności w tej dziedzinie, oraz zdecydowanie wspierała europejskie badania i różnorodność przedsiębiorstw. EKES uważa, że ważne jest zwiększenie zasobów wspólnotowych na rzecz cyfrowych badań naukowych i innowacji oraz wspieranie inwestycji operatorów i dostawców w zakresie nowych funkcjonalności technicznych w dziedzinie bezpieczeństwa, które powinny iść w parze z zdolnością rynku do uznawania i wynagradzania wszystkich inicjatyw mających na celu zwiększenie bezpieczeństwa i odporności systemów.

1.8. Ważne jest zapewnienie bezpieczeństwa wszystkim państwom członkowskim, w tym poprzez utrzymywanie ośrodków badawczych na wielu obszarach w UE: EKES podtrzymuje również swoją sugestię, by było co najmniej dwóch dostawców dla każdego kraju, z których przynajmniej jeden pochodziłby z kraju europejskiego, co mogłoby zagwarantować bezpieczeństwo polityczne danych oraz poszanowanie ograniczeń zdrowotnych.

1.9. EKES uważa, że należy położyć większy nacisk na problem ograniczonych i nieskutecznych instrumentów dla użytkowników, obywateli i odpowiednich organizacji społeczeństwa obywatelskiego, oprócz słusznego skupienia się na właściwych środkach dotyczących uprawnień krajowych organów regulacyjnych i roli operatorów telekomunikacyjnych w celu promowania wzmocnienia pozycji i zdolności konsumentów, tak aby stali się proaktywnymi uczestnikami rynku.

1.10. Komisja Europejska, Parlament Europejski, Rada oraz rządy i parlamenty państw członkowskich muszą zapewnić demokratyczne ramy konsultacji, w których będą mogły być podawane do publicznej wiadomości tematy naukowe lub technologiczne, gwarancje prawne i odpowiedzi właściwych instytucji na pytania społeczeństwa obywatelskiego.

1.11. EKES zaleca wzmocnienie dyplomacji europejskiej w dziedzinie technologii, tak aby zapewnić większą równowagę i wzajemność w dziedzinie handlu i inwestycji, w szczególności w odniesieniu do dostępu do rynku, dotacji, zamówień publicznych, transferu technologii, własności przemysłowej oraz norm społecznych i środowiskowych.

2. **Wprowadzanie**

2.1. Bezpieczeństwo sieci 5G ma znaczenie strategiczne dla obywateli i przedsiębiorstw, całego jednolitego rynku i suwerenności technologicznej UE. Już w 2013 r. Komisja uruchomiła inicjatywę przewodnią UE ustanawiającą partnerstwo publiczno-prywatne 5G (PPP 5G) w celu przyspieszenia badań i innowacji w dziedzinie technologii 5G.

2.2. Technologia 5G, która w 2025 r. będzie według szacunków generować w skali globalnej przychody przekraczające 100 mld euro, stanowi kluczowy atut Europy, który pozwoli jej konkurować na światowych rynkach, a cyberbezpieczeństwo ma decydujące znaczenie dla zapewnienia strategicznej autonomii Unii.

2.3. Sieci 5G opierają się na obecnej 4. generacji (4G) technologii sieciowych i na infrastrukturze światłowodowej, zapewniają nowe zdolności w zakresie usług oraz stają się infrastrukturą o głównym znaczeniu i czynnikiem wspomagającym dla dużej części gospodarki Unii, tworząc trzon szerokiego zakresu usług niezbędnych dla funkcjonowania rynku wewnętrznego oraz utrzymania ważnych funkcji gospodarczych i społecznych, takich jak energetyka, transport, bankowość i usługi zdrowotne oraz rolnicze i przemysłowe systemy produkcji, dystrybucji i konsumpcji, a także zarządzania nimi.

2.4. Biorąc pod uwagę kluczową rolę sieci 5G w transformacji cyfrowej gospodarki i społeczeństwa UE oraz wzajemnie połączony i ponadnarodowy charakter infrastruktur leżących u podstaw ekosystemu cyfrowego oraz transgraniczny charakter tych zagrożeń, wszelkie istotne luki lub incydenty cybernetyczne mające wpływ na sieci 5G i występujące w danym państwie członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G.

2.5. W 2016 r. KE – w ramach zestawu inicjatyw, poczynając od komunikatu „Łączność dla konkurencyjnego rynku cyfrowego: w kierunku europejskiego społeczeństwa gigabitowego” ([1]) ([2]) oraz wniosków w sprawie rozporządzenia ustanawiającego Europejski kodeks łączności elektronicznej ([3]), ustanawiającego Organ Europejskich Regulatorów Łączności Elektronicznej – BEREC ([4]), w sprawie priorytetów w normalizacji ICT na jednolitym rynku cyfrowym ([5]), w sprawie propagowania łączności internetowej w społecznościach lokalnych ([6]) – przyjęła plan działania UE na rzecz sieci 5G ([7]), w sprawie którego EKES wydał pozytywną opinię ([8]), w celu wzmocnienia wysiłków UE na rzecz wdrożenia infrastruktury i usług 5G na jednolitym rynku cyfrowym za pomocą planu działania na rzecz publicznych i prywatnych inwestycji w infrastrukturę sieci 5G w UE oraz celu dotyczącego uruchomienia sieci komercyjnych 5G do 2020 r.

2.6. Zgodnie z definicją zawartą w zaleceniu KE ([9]) „sieci 5G” oznaczają „zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności mobilnej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń”.

2.7. W zaleceniu wyjaśniono, że KE będzie wspierać wdrażanie unijnego podejścia do cyberbezpieczeństwa sieci 5G i – zgodnie z wnioskiem państw członkowskich – będzie działać na rzecz zapewnienia bezpieczeństwa infrastruktury 5G i łańcucha dostaw, wykorzystując, w stosownych przypadkach, wszystkie instrumenty, którymi dysponuje:

— przepisy dotyczące telekomunikacji, multimediów i cyberbezpieczeństwa,

— koordynację normalizacji i certyfikacji na szczeblu UE,

— ramy monitorowania bezpośrednich inwestycji zagranicznych w celu ochrony europejskiego łańcucha dostaw w zakresie sieci 5G,

— instrumenty ochrony handlu,

— reguły konkurencji,

— zamówienia publiczne zapewniające należyte uwzględnienie aspektów bezpieczeństwa,

— programy finansowania UE zapewniające, że beneficjenci spełniają odpowiednie wymogi w zakresie bezpieczeństwa.

2.8. W lipcu 2019 r. państwa członkowskie przedstawiły grupie współpracy ustanowionej na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji ([10]) (złożonej z przedstawicieli każdego państwa członkowskiego), KE i ENISA wyniki krajowych ocen ryzyka zawierające informacje na temat głównych działań, zagrożeń i luk zgodnie z normą ISO/IEC 27005, w odniesieniu do infrastruktury 5G i głównych scenariuszy ryzyka, opisując potencjalne sposoby niepożądanego wykorzystania luk w ramach danego działania. Te krajowe oceny stanowiły podstawę kolejnej skoordynowanej oceny i wspólnego zestawu możliwych środków zmniejszających ryzyko.

2.9. W październiku 2019 r. grupa współpracy ds. bezpieczeństwa sieci i informacji, przy wsparciu Komisji Europejskiej i Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji, opublikowała sprawozdanie na temat skoordynowanej, ogólnounijnej oceny zagrożeń w zakresie cyberbezpieczeństwa w sieciach 5G, w którym wskazano szereg istotnych wyzwań w zakresie bezpieczeństwa związanych z kluczowymi innowacjami technologicznymi oprogramowania, aplikacji i usług, a także rolą dostawców we wdrażaniu i wykorzystywaniu sieci 5G oraz stopniem zależności od poszczególnych dostawców:

— zwiększone narażenie na ataki i zwiększoną liczbę potencjalnych punktów dostępu dla sprawców tych ataków,

— większą wrażliwość ze względu na nowe cechy i funkcjonalności sieci 5G,

— zagrożenia związane z zależnością operatorów sieci komórkowych od dostawców, przy zwiększeniu liczby możliwych dróg ataków ze strony sprawców,

---

([1]) Art. 168 ust. 1 TFUE „Działanie Unii, które uzupełnia polityki krajowe…”.
([2]) COM(2016) 587.
([3]) COM(2016) 590.
([4]) COM(2016) 591.
([5]) COM(2016) 176.
([6]) COM(2016) 589.
([7]) COM(2016) 588.
([8]) Dz.U. C 125 z 21.4.2017, s. 74.
([9]) Zalecenie Komisji (UE) 2019/534 z 26 marca 2019 r. „Cyberbezpieczeństwo sieci 5G” (Dz.U. L 88 z 29.3.2019, s. 42).
([10]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

— znaczenie profilu ryzyka poszczególnych dostawców dla ewentualnej ingerencji spoza UE,

— zwiększone ryzyko spowodowane dużym uzależnieniem od dostawców w związku z zakłóceniami dostaw spowodowanymi napięciami handlowymi lub innymi,

— zagrożenia dla dostępności i integralności sieci w odniesieniu do bezpieczeństwa, poufności i prywatności.

2.10. Wszystkie te wyzwania tworzą nowy model bezpieczeństwa, który sprawia, że konieczna jest ponowna ocena obecnych ram polityki i polityki bezpieczeństwa mających zastosowanie do tego sektora i jego ekosystemu oraz wymaga od państw członkowskich podjęcia niezbędnych środków łagodzących.

2.11. 21 listopada 2019 r. komisja ENISA opublikowała sprawozdanie zatytułowane „Panorama zagrożeń dla sieci 5G", które zawierało ocenę zagrożeń związanych z piątą generacją mobilnych sieci telekomunikacyjnych i stanowiło uzupełnienie sprawozdania państw członkowskich UE.

2.12. 29 stycznia 2020 r. grupa współpracy ds. bezpieczeństwa sieci i informacji opublikowała unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G ([11]) wraz z ewentualnym wspólnym zestawem środków mogących złagodzić poważne zagrożenia dla cyberbezpieczeństwa sieci 5G, zawierającym wytyczne dotyczące wyboru środków, które powinny być traktowane priorytetowo w planach ograniczania ryzyka na szczeblu krajowym i unijnym. W tym samym dniu KE przyjęła komunikat popierający zestaw narzędzi ([12]), który jest przedmiotem tej opinii.

2.13. Główne zainteresowane strony w kontekście sieci 5G to:

— obywatele, konsumenci i użytkownicy końcowi 5G,

— operatorzy sieci łączności ruchomej: podmioty świadczące usługi sieci ruchomych na rzecz użytkowników, zarządzające siecią z pomocą osób trzecich,

— dostawcy operatorów sieci łączności ruchomej: podmioty świadczące usługi lub oferujące infrastrukturę operatorom sieci ruchomych w celu budowy lub eksploatacji ich sieci; kategoria ta obejmuje: producentów sprzętu telekomunikacyjnego, innych dostawców będących stronami trzecimi, takich jak dostawcy infrastruktury w chmurze, integratorów systemów, wykonawców ds. bezpieczeństwa i obsługi technicznej, producentów urządzeń przesyłowych,

— producentów urządzeń połączonych i powiązanych z nimi dostawców usług: podmioty, które dostarczają sprzęt lub świadczą usługi, które będą podłączone do sieci 5G (np. smartfony, pojazdy podłączone do sieci, e-zdrowie) i powiązane komponenty usług, które zostaną uwzględnione w planie kontroli 5G, jak określono w architekturze opartej na usługach lub architekturze Mobile Edge Computing,

— inne zainteresowane strony, w tym dostawcy usług i treści.

Wszystkie te zainteresowane strony są ważnymi podmiotami w dziedzinie bezpieczeństwa, zarówno pod względem przyczyniania się do cyberbezpieczeństwa sieci 5G, jak i potencjalnych punktów wejścia lub wektorów ataku. Ważne jest zatem, aby ocenić ryzyko związane z ich pozycją w ekosystemie 5G.

2.14. Główne tradycyjne kategorie zagrożeń są związane z zagrożeniem poufności, integralności i dostępności. Stwierdzono, że szereg scenariuszy zagrożenia dla sieci 5G dotyczy w szczególności:

— zakłócenia lokalnej lub globalnej sieci 5G (dostępność),

— szpiegostwa w zakresie danych dotyczących ruchu w infrastrukturze sieciowej 5G (poufność),

— modyfikacji lub przekierowania danych w infrastrukturze sieciowej 5G (integralność i/lub poufność),

— zniszczenia lub zmiany innej infrastruktury cyfrowej lub cyfrowych systemów informatycznych za pośrednictwem sieci 5G (integralność i/lub dostępność).

2.15. Zagrożenia stwarzane przez państwa lub podmioty wspierane przez państwo postrzegane są jako niezwykle istotne, ponieważ to najpoważniejsze i najbardziej prawdopodobne podmioty zagrożeń, które mogą mieć powody, intencję, a przede wszystkim zdolność do przeprowadzania uporczywych i wyrafinowanych ataków na bezpieczeństwo sieci 5G.

([11]) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu-toolbox-risk-mitigating-measures
([12]) https://ec.europa.eu/digital-single-market/en/news/secure-5 g-deployment-eu-implementing-eu-toolbox-communication-commission

Chociaż wiele z tych luk nie jest cechą wyłącznie sieci 5G, prawdopodobne jest, że ich liczba i znaczenie wzrosną wraz z 5G ze względu na wyższy poziom złożoności technologii oraz rosnące oczekiwania gospodarek i społeczeństw w tej dziedzinie.

2.16. W szczególności, ponieważ sieci 5G będą w dużej mierze opierać się na oprogramowaniu, główne wady w zakresie bezpieczeństwa, takie jak wady wynikające ze niewłaściwych procesów opracowywania oprogramowania u dostawców, mogłyby ułatwić podmiotom celowe wprowadzanie intencjonalnie wbudowanych luk bezpieczeństwa typu „backdoor" i sprawić, że staną się one jeszcze trudniejsze do wykrycia. Może to zwiększyć ich potencjał do wykorzystania ze szczególnie poważnymi konsekwencjami dotykającymi dużej liczby użytkowników. Kwestie związane z cyberbezpieczeństwem sieci 4G nie zostały jeszcze w pełni rozwiązane, a problemy dotyczące 5G mogą rosnąć wykładniczo.

2.17. Należy także rozważyć luki związane z procesami lub konfiguracją:

— brak wyspecjalizowanych i wyszkolonych pracowników, którzy zajmowaliby się ochroną, monitorowaniem i utrzymywaniem sieci 5G,

— niedociągnięcia w zakresie odpowiednich kontroli bezpieczeństwa wewnętrznego, praktyk w zakresie monitorowania, systemów zarządzania bezpieczeństwem oraz słabe punkty w praktykach zarządzania ryzykiem,

— nieodpowiednie procedury ochrony lub utrzymania dobrego stanu technicznego systemu, takie jak modernizacja oprogramowania/zarządzanie pakietami naprawczymi w sieciach 5G,

— niestosowanie się do standardów 3GPP lub ich niewłaściwe stosowanie,

— niedoskonałości rozwiązań projektowych lub w zakresie architektury sieci, w tym brak skutecznych mechanizmów awaryjnych i zapewniających ciągłość, niewłaściwa lub nieprawidłowa konfiguracja, na przykład w dziedzinie wirtualizacji lub zarządzania prawami dostępu,

— nieodpowiednie kryteria lokalnego i zdalnego dostępu do elementów sieci,

— niewystarczające wymogi dotyczące bezpieczeństwa w procesie zapewniania dostawy usług i produktów; niedociągnięcie to może przyjąć formę niewłaściwych strategii wyboru dostawcy lub nieprzyznania pierwszeństwa kryterium bezpieczeństwa ponad innymi aspektami.

2.18. Profile ryzyka poszczególnych dostawców należy oceniać na podstawie szeregu czynników, w szczególności: możliwości, że dostawca będzie poddany ingerencji z kraju poza UE, czemu sprzyjałyby silne powiązania między dostawcą a rządem danego państwa trzeciego, prawodawstwa państwa trzeciego – w szczególności w przypadku braku legislacyjnych lub demokratycznych mechanizmów kontroli i równowagi, w wyniku czego filie przedsiębiorstwa działające w UE mogłyby być nakłaniane do nieprzestrzegania prawodawstwa unijnego – lub w przypadku braku umów o bezpieczeństwie lub ochrony danych między UE a danym państwem trzecim, struktury własnościowej dostawcy, zdolności państwa trzeciego do wywierania jakiegokolwiek nacisku, w tym odnośnie do miejsca produkcji sprzętu, ogólnej jakości produktów i praktyk stosowanych przez dostawcę w zakresie cyberbezpieczeństwa, w tym stopnia kontroli nad jego łańcuchem dostaw oraz odpowiednich priorytetów w zakresie bezpieczeństwa.

2.19. Państwa członkowskie uzgodniły zapewnienie odpowiednich i proporcjonalnych środków w odniesieniu do wskazanych już i możliwych przyszłych zagrożeń. Uzgodniły w szczególności, że będą w stanie ograniczyć lub nałożyć szczegółowe wymogi i warunki w ramach podejścia opartego na analizie ryzyka w odniesieniu do dostarczania, dystrybucji i eksploatacji urządzeń sieciowych 5G lub też ich zakazać.

2.20. W tym celu państwa członkowskie powinny:

— zaostrzyć wymogi w zakresie bezpieczeństwa w odniesieniu do operatorów sieci ruchomych, takie jak rygorystyczne kontrole dostępu, zasady bezpiecznej eksploatacji i monitorowania, ograniczenia w outsourcingu konkretnych funkcji,

— ocenić na podstawie obiektywnych i jasnych kryteriów profil ryzyka dostawców oraz w związku z tym, kierując się zasadami proporcjonalności i pewności prawa, stosować odpowiednie ograniczenia w odniesieniu do dostawców wysokiego ryzyka, w tym niezbędne wyłączenia w celu skutecznego ograniczania ryzyka związanego z aktywami kluczowymi i wrażliwymi określonymi w skoordynowanej ocenie ryzyka na szczeblu UE,

— przyjąć ogólnie uznane i wdrażane oraz oparte na konsensusie standardy i najlepsze praktyki w zakresie bezpieczeństwa,

— zagwarantować, że każdy operator ma odpowiednia strategię wielu dostawców, tak aby uniknąć uzależniania się od jednego dostawcy lub dostawców o podobnym profilu ryzyka lub też ograniczyć taką sytuację,

— zapewnić ścisłą kontrolę dostępu oraz bezpieczne zarządzanie sieciami oraz ich działanie i monitorowanie wraz z korzystaniem z certyfikacji dla elementów i/lub procesów sieci 5G; strategia ta musi opierać się na analizie ryzyka przeprowadzanej przez państwa członkowskie i operatorów, tak aby wybór strategii wielu dostawców nie spowodował zwiększenia poziomu ryzyka dla sieci operatora,

— zapewnić odpowiednią równowagę dostawców na szczeblu krajowym i unikać uzależnienia od dostawców ocenianych jako prezentujący wysoki poziom ryzyka, również poprzez promowanie większej interoperacyjności sprzętu,

— utrzymać zróżnicowany i zrównoważony łańcuch dostaw 5G w celu uniknięcia długotrwałej zależności, przy pełnym wykorzystaniu unijnych instrumentów kontroli bezpośrednich inwestycji zagranicznych, instrumentów ochrony handlu, dyscypliny konkurencji oraz przepisów UE dotyczących zamówień publicznych,

— wzmocnić wewnętrzne zdolności UE w dziedzinie technologii 5G i technologii będącej następcą 5G z wykorzystaniem odpowiednich funduszy i programów UE, zapewnić koordynację działań państw członkowskich w dziedzinie normalizacji poprzez wzmocnienie zdolności „testu" i „audytu" w celu realizacji określonych celów w zakresie bezpieczeństwa oraz opracowania odpowiednich systemów certyfikacji UE na mocy aktu o cyberbezpieczeństwie, a także propagowania interoperacyjności.

2.21. Jak wielokrotnie podkreślała KE, europejski rynek wewnętrzny jest i pozostaje otwarty dla podmiotów pragnących przybyć do Europy, o ile wszystkie spełnią jasne i wymagające przepisy oparte na obiektywnych kryteriach.

2.22. W dniu 6 czerwca 2020 r. Rada podkreśliła znaczenie wzmocnienia suwerenności cyfrowej i współpracy cyfrowej w UE, a także stworzenia synergii poprzez unijne programy, takie jak instrument „Łącząc Europę" i program „Cyfrowa Europa", wraz z rozwojem umiejętności cyfrowych, rozwojem gospodarki opartej na danych, podkreśleniem znaczenia sztucznej inteligencji i cyberbezpieczeństwa oraz aktywną rolą sektora cyfrowego w osiąganiu celów Zielonego Ładu.

3. **Komunikat Komisji**

3.1. W odpowiedzi na zestaw narzędzi bezpieczeństwa dla sieci 5G opracowany przez grupę współpracy ds. bezpieczeństwa sieci i informacji Komisja:

— zobowiązuje się dołożyć wszelkich starań, na wniosek państw członkowskich, na rzecz zapewnienia bezpieczeństwa infrastruktury 5G i łańcucha dostaw, z wykorzystaniem, w stosownych przypadkach, wszystkich instrumentów, którymi dysponuje,

— wzywa państwa członkowskie do zapewnienia wdrożenia skutecznych strategii ograniczania ryzyka oraz do podjęcia na szczeblu UE dalszych środków koordynacji w zakresie wspólnego podejścia do cyberbezpieczeństwa sieci 5G,

— zachęca państwa członkowskie do kontynuowania wdrażania zestawu środków zalecanych w konkluzjach w sprawie pakietu instrumentów oraz do przygotowania wspólnego sprawozdania na temat ich wdrażania, podczas gdy grupa ds. współpracy w zakresie bezpieczeństwa sieci i informacji będzie kontynuować prace mające na celu wspieranie wdrażania zestawu narzędzi,

— określa – w sektorach wchodzących w zakres jej kompetencji – działania mające na celu zapewnienie cyberbezpieczeństwa sieci 5G i zdywersyfikowanego łańcucha wartości 5G, normalizacji technicznej i certyfikacji, bezpośrednich inwestycji zagranicznych i ochrony handlu oraz konkurencji, zamówień publicznych i dyplomacji cyfrowej, a także ich własnych programów i funduszy istotnych z punktu widzenia badań naukowych i innowacji, spójności i rozwoju.

4. **Uwagi ogólne**

4.1. EKES jest przekonany, że nowe technologie 5G są w stanie zmienić sposób interakcji ze światem, oferując możliwości takie jak nowe aplikacje, modele biznesowe, nowy styl życia, inteligentne fabryki, większa wydajność i nowe wysokiej jakości usługi dla obywateli, potencjalnie otwierając dostęp do przełomowych technologii, takich jak zautomatyzowane samochody oraz zaawansowane systemy produkcji i dystrybucji, a także umożliwiając wielu tysiącom połączonych ze sobą urządzeń wejście w nasze codzienne życie w ramach internetu rzeczy. EKES chciałby jednak, by Komisja wzmocniła analizy wpływu i wykonalności oraz analizy kosztów i korzyści w odniesieniu do technologii 5G w porównaniu z wykorzystaniem technologii 4G lub telekomunikacji światłowodowej. EKES uważa, że istotne jest, by strategia 5G była ukierunkowana na osiągnięcie lepszego wykorzystania zasobów w obiegu zamkniętym i zmniejszenie dużego śladu węglowego związanego z energią. EKES podkreśla, jak ważne jest uwzględnienie społecznych zmian strukturalnych poprzez wzmocnienie sprawiedliwej i płynnej transformacji oraz rozwiązanie problemu niedoboru kwalifikacji w celu uzyskania lepiej płatnych, elastycznych i wysoko wykwalifikowanych miejsc pracy.

4.2. To trojakie zagrożenie – niekontrolowane pandemie, niewystarczający zestaw środków polityki gospodarczej oraz zjawiska typu „czarny łabędź" na płaszczyźnie geopolitycznej – może wpędzić światową gospodarkę w stałą depresję i prowadzić do krachów finansowych i ucieczki kapitału z rynku finansowego właśnie wtedy, gdy wszystkie grupy społeczeństwa europejskiego nabywają coraz większą świadomość, że zrównoważony rozwój gospodarczy i **obecna rewolucja cyfrowa – której fundamentem jest 5G** – wymagają sposobów jednoczesnego połączenia suwerenności technologicznej, wzrostu wydajności i bardziej efektywnego wykorzystania dostępnych zasobów, wspieranych przez odpowiednie ramy prawne i regulacyjne oraz ramy gospodarcze i finansowe.

4.3. EKES wzywa instytucje UE i państwa członkowskie do ukończenia tworzenia jednolitego rynku cyfrowego, m.in. poprzez budowanie zdolności w zakresie integracji i wykorzystania usług 5G w celu ochrony i poprawy konkurencyjności europejskiego przemysłu. Wzywa państwa członkowskie do dalszego przyspieszenia tego procesu, z uwzględnieniem wszystkich aspektów bezpieczeństwa i ochrony, w tym aspektów dotyczących wpływu technologii 5G na zdrowie publiczne i żywe ekosystemy, wpływu na sytuację społeczno-gospodarczą i konkurencję, wpływu na kształcenie i szkolenia oraz gwarancję poszanowania praw podstawowych, takich jak prawo własności lub prawo do prywatności i bezpieczeństwa danych osobowych.

4.4. EKES apeluje, by UE stała się światowym liderem w dziedzinie technologii mobilnej kolejnej generacji 5G wyposażonej w bezpieczną infrastrukturę cyfrową stanowiącą solidną podstawę nowej, nowoczesnej europejskiej strategii przemysłowej poprzez radykalną zmianę w zakresie łączności mobilnej oraz posiadającą ogromny, dynamiczny potencjał na rzecz zwiększenia wydajności i rozwoju gospodarki oraz usług dla obywateli, ich dobrobytu, a także ochrony klimatu i środowiska, dzięki czemu UE stanie się liderem rewolucji 5G.

4.5. Biorąc pod uwagę, że cyberbezpieczeństwo i bezpieczeństwo narodowe są ze sobą nierozerwalnie związane, EKES uważa, że wszelkie decyzje w sprawie bezpieczeństwa narodowego państwa członkowskiego UE muszą być podejmowane w kontekście UE, oraz że oceny nietechniczne powinny być przeprowadzane obiektywnie na podstawie kryteriów oceny ryzyka określonych na szczeblu europejskim, niezbędnych do zapewnienia zharmonizowanego i przewidywalnego otoczenia regulacyjnego w całej Europie, które zapewni pełną interoperacyjność.

4.6. EKES uważa, że jakość informacji i sposób ich przekazywania – tzw. efekt sformułowania, tzn. efekt związany z kontekstem lub uwidocznieniem danego elementu – mają istotny wpływ na zachowanie odbiorców. Cel, jakim jest promowanie wzmocnienia pozycji konsumentów, jest zatem odzwierciedlony w określaniu narzędzi służących edukacji i wzmacnianiu pozycji konsumentów jako uczestników rynku cyfrowego. EKES uznaje potrzebę dostarczania obywatelom aktualnych i prawidłowych informacji na temat korzyści i zagrożeń związanych z 5G w oparciu o konsensus zdecydowanej większości środowiska naukowego i wskazuje na te aspekty, co do których taki konsensus jest niepewny.

4.7. EKES jest przekonany, że dostęp do europejskiego rynku cyfrowego powinien być nadal otwarty dla każdego przedsiębiorstwa bez dyskryminacji, ale w ramach europejskich zasad, norm i solidnych, jasnych kryteriów oceny i bezpieczeństwa, stawiających w centrum strategii europejskiej odzyskanie i ożywienie europejskiej suwerenności technologicznej.

4.8. Chociaż wśród pięciu głównych dostawców infrastruktury znajduje się dwóch dostawców europejskich, dwóch chińskich i jeden koreański ([13]), żadne duże przedsiębiorstwo europejskie nie należy do pierwszych, które produkuje urządzenia i zestawy układów scalonych 5G; EKES jest głęboko przekonany, że należy zagwarantować pluralizm dostawców, z których przynajmniej jeden jest własnością europejskiej spółki dominującej, a także ramy interoperacyjności i pełną zamienność elementów sprzętu i oprogramowania, również w celu zapewnienia pełnej europejskiej suwerenności technologicznej w kontekście ścisłej współpracy międzynarodowej i pełnej wzajemności w zakresie otwartości, dostępu i działania na rynkach. Takie zróżnicowanie może być stosowane, o ile możliwa jest interoperacyjność usług, a różnorodność nie zwiększa zagrożeń z punktu widzenia cyberbezpieczeństwa.

4.9. EKES uważa za niezbędne, by Europa przyjęła średnioterminową wizję autonomii i samowystarczalności w tej dziedzinie, oraz zdecydowanie wspiera europejskie badania i różnorodność przedsiębiorstw. EKES z zadowoleniem przyjmuje pakiet środków uzgodnionych przez państwa członkowskie w celu przeciwdziałania zagrożeniom dla bezpieczeństwa i ochrony związanym z wprowadzeniem technologii 5G, które zostały już określone w ocenie europejskiej. Uważa jednak, że rygorystyczne i bezpieczne wartości graniczne ekspozycji na pola elektromagnetyczne, zalecane na poziomie UE i oparte na aktualnych wytycznych Międzynarodowej Komisji Ochrony przed Promieniowaniem Niejonizującym (ICNIRP), uznanych przez Światową Organizację Zdrowia (WHO), powinny mieć zastosowanie do wszystkich pasm częstotliwości 5G ([14]): wartości graniczne ICNIRP opierają się na zasadzie ostrożności, ponieważ są 50 razy niższe niż poziomy wpływu na zdrowie publiczne ustalone na podstawie dostępnych dowodów naukowych.

([13]) Grupę pięciu dostawców światowych tworzą obecnie: Ericsson, Nokia, Huawei, ZTE i Samsung.
([14]) PE – E-003040/2019 – Odpowiedź udzielona przez Stellę Kyriakides w imieniu Komisji Europejskiej (17 stycznia 2020 r.).

4.10. EKES zauważa jednak, że ICNIRP nie jest uznawany przez całą społeczność naukową, a niektórzy naukowcy promują znacznie bardziej rygorystyczne dopuszczalne wartości narażenia ludności zgodnie z zasadą ALARA (na najniższym racjonalnie osiągalnym poziomie). Rozwiązania, które można by zaproponować jako uzupełnienie infrastruktury komunikacyjnej 5G, obejmują wykorzystanie stałych łączy transmisji danych przez istniejące technologie nieradiowe (kable Ethernet, światłowody itp.), w sytuacjach, gdy ich wykorzystanie jest stałe (np. bankomaty, oddziały banków, roboty przemysłowe, zdalnie sterowane roboty medyczne itp.) oraz tam, gdzie działają duzi użytkownicy przesyłu danych (dostawcy usług cyfrowych, firmy/przedsiębiorstwa itp.); internet rzeczy znajdujących się w stałych, niemobilnych lokalizacjach (inteligentny dom, inteligentne miasto, czujniki w urządzeniach użyteczności publicznej itp.).

4.11. Komisja Europejska, Parlament Europejski, Rada oraz rządy i parlamenty państw członkowskich muszą zapewnić demokratyczne ramy konsultacji, w których będą mogły być podawane do publicznej wiadomości tematy naukowe lub technologiczne, gwarancje prawne i odpowiedzi właściwych instytucji na pytania społeczeństwa obywatelskiego.

4.12. EKES uważa, że należy położyć większy nacisk na ograniczone i nieskuteczne instrumenty dla użytkowników, obywateli i odpowiednich organizacji społeczeństwa obywatelskiego, a także słusznie skoncentrować się na odpowiednich środkach dotyczących uprawnień krajowych organów regulacyjnych i na roli operatorów telekomunikacyjnych.

4.13. EKES uznał ([15]) istnienie problemu nadwrażliwości elektromagnetycznej (EHS) i podkreślił swoje obawy, uznając za zachęcający fakt, iż prowadzone są dalsze szczegółowe badania mające na celu zrozumienie problemu i jego przyczyn, a także wzywa Komisję do kontynuowania i aktualizacji prac w tej dziedzinie.

4.14. Wiarygodność dostawców usług telekomunikacyjnych i zastosowań 5G ma, zdaniem EKES-u, zasadnicze znaczenie, ponieważ zarządzanie informacjami w internecie stanowi podstawę usług w zakresie agregacji danych gromadzonych i przetwarzanych przez użytkowników za pomocą mechanizmów technologicznych, prawnych i podatkowych, łączących ze sobą bezpośrednio obiekty, maszyny i algorytmy.

4.15. EKES zaproponował ([16]) przejście od koncepcji własności danych do definicji praw do danych dla osób fizycznych i prawnych. Konsumenci powinni mieć kontrolę nad danymi wytwarzanymi przez połączone urządzenia, w sposób zapewniający ochronę prywatności konsumentów wraz z dostępnością, interoperacyjnością i przekazywaniem danych, przy jednoczesnym zapewnieniu odpowiedniej ochrony danych i poufności, uczciwej konkurencji i szerszego wyboru dla konsumentów.

4.16. Ogólne rozporządzenie o ochronie danych (RODO) powinno zostać wzbogacone o jasne wytyczne dotyczące wdrażania w celu osiągnięcia jednolitego stosowania i wysokiego poziomu ochrony danych oraz ochrony konsumentów w świetle wzajemnych połączeń maszyn i przedmiotów oraz zmiany przepisów dotyczących odpowiedzialności cywilnej i ubezpieczenia produktów, w celu dostosowania ich do sytuacji, w której decyzje będą w coraz większym stopniu podejmowane przez oprogramowanie w całkowicie bezpiecznym środowisku.

4.17. EKES uważa za niezbędne, by państwa członkowskie stosowały się do strategicznych i technicznych zaleceń zawartych w zestawie narzędzi UE, unikając opracowywania konkretnych podejść krajowych, takich jak dodatkowe testy i certyfikacja, które prowadziłyby do fragmentacji rynku, opóźnień we wdrażaniu technologii i niespójności między rynkami, co groziłoby podważeniem zaufania do systemów testowania i certyfikacji.

4.18. EKES uważa, że konieczne jest stosowanie norm światowych, przy większym wsparciu ze strony Europy, oraz wspólnych i uznanych sprawdzonych rozwiązań w celu umożliwienia skutecznego zarządzania zagrożeniami, uzyskania korzyści skali, uniknięcia fragmentacji i zapewnienia interoperacyjności systemów europejskich. Rozmowy na temat norm technicznych są niezbędnym wyjaśnieniem, które pozwoli przedsiębiorstwom na ponowne podjęcie konkurencji i prowadzenie tych kluczowych działań w celu wdrożenia zaawansowanych technologii, takich jak 5G i sztuczna inteligencja (SI), na wszystkich rynkach.

4.19. W szczególności EKES uważa, że zasadnicze znaczenie ma zapewnienie oceny ryzyka dla dostawców oraz stosowanie odpowiednich ograniczeń w odniesieniu do dostawców wysokiego ryzyka, w tym niezbędnych wyłączeń w celu skutecznego ograniczenia ryzyka związanego z aktywami kluczowymi i wrażliwymi określonymi w skoordynowanej ocenie ryzyka na szczeblu UE.

4.20. EKES uważa, że istotne jest zwiększenie inwestycji operatorów i dostawców w zakresie nowych funkcjonalności technicznych w dziedzinie bezpieczeństwa, które powinny iść w parze z zdolnością rynku do uznawania i wynagradzania wszystkich inicjatyw mających na celu zwiększenie bezpieczeństwa i odporności systemów. Większa koncentracja na inwestycjach w bezpieczeństwo mogłaby przynieść nowe korzyści rynkowe.

([15]) Dz.U. C 242 z 2.7.2015, s. 31.
([16]) Dz.U. C 353 z 18.10.2019, s. 79.

4.21. EKES zdecydowanie popiera wspólne działania na rzecz wspierania rozwoju przemysłowego i wdrażania sieci 5G: ocenę potencjalnych niepowodzeń lub luk rynkowych w łańcuchu wartości 5G, uzasadniającą ukierunkowane interwencje w następnym długoterminowym budżecie lub ewentualny projekt stanowiący przedmiot wspólnego europejskiego zainteresowania w zakresie cyberbezpieczeństwa 5G (bezpieczeństwa i ochrony).

4.22. EKES podkreśla, że chociaż infrastruktura cyfrowa okazała się odporna i solidna w czasie kryzysu wywołanego przez COVID-19, konieczne są dalsze inwestycje w infrastrukturę 5G w celu przezwyciężenia wciąż istniejącej przepaści cyfrowej, która może ograniczyć dostęp obywateli do e-zdrowia, e-nauki i pracy zdalnej.

4.23. Jeśli chodzi o dyplomację technologiczną, EKES uważa, że zasadnicze znaczenie ma zapewnienie przez UE bardziej zrównoważonych i wzajemnych warunków dla handlu i inwestycji, w szczególności w zakresie dostępu do rynku, dotacji, zamówień publicznych, transferu technologii, własności przemysłowej oraz norm społecznych i środowiskowych, zwłaszcza w obecności „systemowych konkurentów promujących alternatywne modele zarządzania", przy jednoczesnym dążeniu do pełnej konkurencji i innowacji technicznych na rynku.

4.24. EKES zdecydowanie popiera potrzebę utrzymania zdywersyfikowanego i zrównoważonego łańcucha dostaw 5G w celu uniknięcia długotrwałej zależności poprzez zapewnienie obecności wielu dostawców w ramach zastępowalności i interoperacyjności oraz dalszego wzmacniania ram finansowych na lata 2021–2027 w odniesieniu do programów i inicjatyw na rzecz budowania zdolności oraz europejskiej suwerenności technologicznej 5G i post-5G.

4.25. W kontekście planu naprawy gospodarczej dla Europy przyjętego w dniu 27 maja 2020 r., Indeks gospodarki cyfrowej i społeczeństwa cyfrowego 2020 (DESI) będzie stanowił źródło informacji dla analiz krajowych wspierających zalecenia agendy cyfrowej zawarte w europejskim semestrze. Pomoże to państwom członkowskim ukierunkować i uszeregować pod względem ważności ich potrzeby w zakresie reform i inwestycji, ułatwiając tym samym dostęp do Europejskiego Instrumentu na rzecz Odbudowy i Zwiększania Odporności o wartości 560 mld EUR. Instrument ten zapewni państwom członkowskim środki, które pozwolą ich gospodarkom zwiększyć odporność oraz zagwarantuje, że inwestycje i reformy będą wspierać przejście na gospodarkę ekologiczną i cyfrową. Ponieważ pandemia wywarła znaczący wpływ na każdy z pięciu wymiarów DESI, wnioski na 2020 r. dotyczące 5G należy odczytywać w powiązaniu z licznymi środkami podejmowanymi przez KE i państwa członkowskie w celu zarządzania kryzysem i wspierania odbudowy gospodarczej.

Bruksela, dnia 16 września 2020 r.

Luca JAHIER
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego