Cen usług telekomunikacyjnych wzrosną o kilkanaście procent

25 kwietnia 2022

Przedsiębiorcy rynku telekomunikacyjnego, prawnicy, eksperci i politycy krytykują tryb procedowania nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Siódma wersja projektu, która pojawiła się w marcu, podobnie jak pięć poprzednich nie została poddana konsultacjom społecznym, mimo wprowadzania do nich istotnych zmian. Krytyka dotyczy szczególnie możliwości wykluczania z rynku pochodzących spoza UE i NATO dostawców sprzętu i usług ICT. Eksperci ostrzegają, że konieczność rezygnacji ze sprzętu danego dostawcy będzie dla operatorów oznaczała spory wydatek. Koszty szacowane na miliardy złotych zostaną ostatecznie przeniesione na konsumentów.

„Prace nad ustawą o cyberbezpieczeństwie trwają od prawie dwóch lat. W tej chwili mamy do czynienia już z siódmą wersją tego projektu. Zgłoszono do tej pory 750 poprawek i praktycznie – oprócz tej początkowej wersji – nie było żadnych konsultacji. Widać, że sposób procedowania tej ustawy jest patologiczny. A to oznacza, że nie może prowadzić do dobrych rezultatów, ponieważ nie uwzględni interesów bardzo dużej grupy polskich przedsiębiorstw" – mówi agencji Newseria Biznes Andrzej Arendarski, prezydent Krajowej Izby Gospodarczej. – Rozumiem, że szczególnie teraz względy bezpieczeństwa są na pierwszym miejscu, ale nie mogą być przykrywką do partactwa legislacyjnego i do pomijania interesariuszy, istotnych z punktu widzenia przyszłego kształtu ustawy.

Ustawa o krajowym systemie cyberbezpieczeństwa (KSC), przyjęta w 2018 roku, to pierwszy w Polsce akt prawny dotyczący tego obszaru. Rząd już od jesieni 2020 roku przymierza się do jej nowelizacji, która ma wzmocnić polskie bezpieczeństwo cybernetyczne. Nowela wpłynie też na kształt całego polskiego rynku telekomunikacyjnego oraz wdrażanie w Polsce sieci 5G i

wybór dostawców infrastruktury dla tej technologii. Prace nad nowelizacją od początku budzą kontrowersje. Zgłoszone w czasie pierwszych – i jedynych konsultacji – uwagi ze strony rynku zostały jednak uwzględnione w stopniu marginalnym, za to w kolejnych wersjach projektu rząd wprowadzał daleko idące zmiany, jak np. pomysł powołania państwowego operatora telekomunikacyjnego. Nie zostały one jednak omówione z rynkiem. Dlatego wątpliwości branży i ekspertów budzą zarówno jego zapisy, jak i tryb procedowania.

„W intencji zapisy tej ustawy mają prowadzić do zwiększenia cyberbezpieczeństwa naszego kraju i szerzej, Unii Europejskiej i NATO, bo jesteśmy częścią tych organizacji. Natomiast sposób, w jaki to jest przeprowadzane, chaos będzie prowadził raczej w kierunku odmiennym. Dlatego jako Krajowa Izba Gospodarcza kilka dni temu wysłaliśmy pismo do premiera, domagając się rzetelnych konsultacji ze wszystkimi interesariuszami rynku telekomunikacyjnego" – mówi Andrzej Arendarski.

Jedną z największych kontrowersji w projektowanej ustawie jest od początku mechanizm oceny profilu ryzyka dostawców sprzętu i usług ICT na polski rynek. Ma jej dokonywać rządowe Kolegium ds. Cyberbezpieczeństwa, które pod uwagę weźmie szereg kryteriów technicznych i nietechnicznych. Zgodnie z najnowszą wersją projektu są wśród nich m.in. certyfikaty oraz liczba i rodzaj wykrytych podatności, ale kolegium uwzględni też to, czy dostawca pochodzi spoza UE lub NATO oraz jakie stwarza ryzyko dla realizacji zobowiązań sojuszniczych i europejskich.

Co ciekawe, w pierwotnej wersji projektu jednym z kryteriów było również to, czy w kraju pochodzenia dostawcy są przestrzegane prawa człowieka, jednak rząd po fali krytyki wycofał się z tego pomysłu. Zdaniem rynku i ekspertów narodowościowe kryteria są bowiem wprost wymierzone w dostawców technologii z Chin.

„Im bardziej radykalna wersja przepisów przejdzie, im krótszy

będzie czas na ewentualną wymianę sprzętu, im więcej dostawców zostanie z rynku wyrzuconych, a mówimy o całym zbiorze różnych firm, które produkują sprzęt w Azji i mogą zostać z tego rynku usunięte, tym większe będą koszty. I tutaj mamy, w mojej ocenie, w tej chwili jedną wielką niewiadomą. Natomiast koszty pośrednie i bezpośrednie wzrosną i to jest coś, z czym wszyscy właściwie eksperci, którzy brali udział w dyskusji Zespołu ds. Ochrony Praw Konsumentów i Przedsiębiorców, się zgadzają, i coś, czego rząd nie uwzględnia w swoich analizach i nie komunikuje tego transparentnie społeczeństwu, ile ta operacja może kosztować" – mówi Krzysztof Bosak, poseł Konfederacji, który uczestniczył w debacie parlamentarnego zespołu, jaka odbyła się 22 kwietnia br. na terenie Sejmu.

Projektowany w ustawie mechanizm oceny jest istotny o tyle, że na jego podstawie – bazując na opinii Kolegium ds. Cyberbezpieczeństwa – minister właściwy ds. informatyzacji będzie mógł podjąć decyzję o uznaniu danego dostawcy za tzw. dostawcę wysokiego ryzyka, czyli podmiot stanowiący „poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego". Nadanie takiego statusu będzie zaś de facto oznaczać wykluczenie z polskiego rynku, bez realnych narzędzi odwoławczych.

„Od tej decyzji nie ma odwołania. To też bardzo dziwi, bo właściwie każde prawo, które w czymś ogranicza przedsiębiorców, powinno mieć swoją drogę odwoławczą. Tutaj takiej drogi nie ma. Decyzja raz podjęta na zawsze wyklucza daną firmę z polskiego rynku telekomunikacyjnego" – zauważa Andrzej Arendarski.

Operatorzy i firmy telekomunikacyjne, które korzystają ze sprzętu i usług dostawcy wysokiego ryzyka, zgodnie z ustawą będą zmuszone pozbyć się ich w ciągu kilku lat. To zaś oznacza dla nich wielomiliardowe koszty, związane choćby z wymianą sprzętu na nowy. Eksperci wskazują, że bez wątpienia odbije się to na cenach usług dla klientów.

„Jeżeli wartość zakupu sprzętu w przypadku budowy infrastruktury 5G na jednego operatora to będą kwoty liczone w setkach milionów złotych, to jeśli wiemy, że jest czterech operatorów, daje nam to wartości liczone w miliardach. Operatorzy nie są instytucjami charytatywnymi. To są firmy obliczone na zysk, osiągnięcie jak najlepszych wyników finansowych – wobec tego te koszty będą musiały zostać rozłożone na klientów, którzy korzystają z ich usług" – mówi prof. dr hab. Maciej Rogalski, rektor Uczelni Łazarskiego. – Można z pewnym założeniem stwierdzić, że ten wzrost cen usług telekomunikacyjnych będzie o co najmniej kilkanaście procent, jeżeli nie więcej.

Do oceny dostawców sprzętu i usług ICT zostali dopuszczeni – po wielomiesięcznych apelach z rynku – operatorzy i firmy telekomunikacyjne. Taką możliwość dostali jednak tylko najwięksi gracze, którzy w poprzednim roku wypracowali obroty w wymaganej ustawą wysokości (równowartość około 113 mln zł). To oznacza, że MŚP będą z tej procedury wykluczone, co de facto pozbawia je możliwości decydowania o kształcie rynku, na którym prowadzą działalność. Jak wskazuje w liście do premiera KIG, o ile ustawa nakłada obowiązek na 4 tys. przedsiębiorców telekomunikacyjnych, o tyle szczególne uprawnienia przyznano tylko kilkunastu.

„W świetle dotychczasowych zapisów projektów ustawy o cyberbezpieczeństwie małe i średnie firmy mogą poczuć się dyskryminowane, ponieważ są wykluczane z procesu decyzyjnego dotyczącego dopuszczenia na polski rynek dostawców sprzętu spoza krajów Unii Europejskiej i NATO" – mówi Andrzej Arendarski. „Trzeba dopuścić do udziału w tym procesie nie tylko te największe firmy, tych gigantów operatorów, ale również przedstawicieli MŚP, choćby w formie izb przemysłowo-handlowych, które zrzeszają takie przedsiębiorstwa".

Eksperci wprost wskazują, że projektowana ustawa o cyberbezpieczeństwie będzie mieć daleko idące konsekwencje ekonomiczne i wpłynie na rozwój polskiego rynku

telekomunikacyjnego w nadchodzących latach, dlatego powinna zostać poddana rzetelnym konsultacjom publicznym. Co istotne, jej kształt może mieć też wpływ na relacje między Polską i Chinami, które – w obawie przed dyskryminacją swoich firm – podejmą działania odwetowe wymierzone w przedsiębiorstwa z Polski.

„Tego rodzaju rozwiązanie, że wyklucza się określone podmioty tylko z tej racji, że pochodzą z innego kraju czy innego obszaru gospodarczego, jest zawsze bardzo ryzykowną operacją z punktu widzenia ekonomicznego, prawnego, podstawowych zasad konkurencji. Wykluczenie określonego dostawcy tylko z tego powodu, że pochodzi z innego kraju, oznacza możliwość wygenerowania problemów o charakterze prawnym z tytułu przepisów obowiązujących w regulacjach unijnych, ale także i umów międzynarodowych, które zakładają wolność, swobodę handlu międzynarodowego. To także ryzyko retorsji ze strony krajów, z których pochodzą ci producenci" – zauważa prof. Maciej Rogalski.

„Jesteśmy zwolennikami dbania o cyberbezpieczeństwo, ale z uwzględnieniem zasad wolności gospodarczej, nieingerowania w rynek bardziej niż to absolutnie niezbędne. A to powinno wynikać z pewnych obiektywnych miar o charakterze technicznym, z wymagań sprzętowych, z certyfikacji sprzętu i stosowanych zabezpieczeń czy też trybu świadczonego wsparcia w przypadku wystąpienia jakichś zagrożeń, incydentów, awarii, naruszeń – mówi Krzysztof Bosak. – W naszym odbiorze ten sposób konstruowania przepisów ma dużo wspólnego z polityką, a bardzo mało z cyberbezpieczeństwem" – zwraca uwagę poseł.

Źródło: Newseria.pl