KRAJOWA IZBA KOMUNIKACJI ETHERNETOWEJ

ul. Lindleya 16, 02-013 Warszawa
tel. + 48 22 2928700, fax +48 22 2928701
www.kike.pl, e-mail: biuro@kike.pl, grap@kike.pl
KRS 0000316678, REGON 141637224, NIP 9512270210

Cz. II

UWAGI SZCZEGÓŁOWE DO STANOWISKA KIKE Z 4.2.2021 DO *USTAWY O ZMIANIE USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA ORAZ USTAWY – PRAWO TELEKOMUNIKACYJNE*

(projekt z dnia 20 stycznia 2021 r. – dalej również jako **Projekt**).

WSTĘP

1. **Nieprzeprowadzenie konsultacji publicznych odnośnie do nowych rozwiązań, zasadnicze modyfikacje ustawy nowelizującej po zakończeniu konsultacji publicznych**

Porównując choćby wizualnie Poprzedni Projekt z Projektem, można zauważyć, że w Projekcie wprowadza się nowe konstrukcje i instytucje prawne, których Poprzedni Projekt nie przewidywał i – tym samym – które nie były wcześniej poddane konsultacjom publicznym. Dobrym przykładem, potwierdzającym zasadność tego spostrzeżenia, jest chociażby zaproponowana zmiana w ustawie *Prawo telekomunikacyjne* (zwanej dalej **UstPT**), polegająca na dodaniu do tego aktu prawnego art. 115^4 (zapewnienie częstotliwości w celu ich oferowania na warunkach hurtowych) czy instytucja polecenia zabezpieczającego i objęcie nią każdego przedsiębiorcy telekomunikacyjnego (art. 67b, który ma zostać wprowadzony do ustawy *o krajowym systemie cyberbezpieczeństwa*, zwanej dalej **UKSC**).

W ocenie KIKE, wprowadzenie tak istotnych i szerokich zmian w ustawie nowelizującej powinno skutkować tym, że **Projekt *de facto* powinien przejść proces legislacyjny od początku**. W szczególności, istotną kwestią byłoby poddanie nowych rozwiązań uzgodnieniom i konsultacjom publicznym. Podmioty biorące udział w konsultacjach publicznych nie miały możliwości odniesienia się do części rozwiązań i mechanizmów przewidzianych w Projekcie. Jeśli choćby pewne etapy realizacji procesu legislacyjnego nie zostaną ponowione odnośnie do nowej wersji ustawy nowelizacyjnej, trzeba będzie rozważać, czy takie podejście do tego tematu nie było działaniem celowym ustawodawcy, a w szczególności, czy nie chodziło o to, aby kontrowersyjne przepisy nie były konsultowane, uzgadniane czy opiniowane.

Wprowadzenie szerokich modyfikacji w ustawie nowelizującej jest wszak widoczne gołym okiem. Objętość Poprzedniego Projektu wynosiła zaledwie 25 stron tekstu, natomiast Projekt ma aż 43 strony (czyli prawie dwa razy więcej). Już tylko na podstawie takiej pobieżnej oceny Projektu, można stwierdzić, że połowa nowych przepisów „ominęła" poprzednią część procesu legislacyjnego, a tym samym, że uniemożliwiono społeczeństwu oraz najbardziej zainteresowanym podmiotom - w tym reprezentowanym przez KIKE operatorom - przedstawienia stanowiska co do jej treści. Takie działania należy ocenić jednoznacznie negatywnie.

Powyższe potwierdza również to, że pomimo chęci zmodyfikowania przepisów UKSC, przed przystąpieniem do zmiany przepisów, ustawodawca nie poświęcił wystarczającego okresu czasu na przemyślenie tego, jaki jest cel modyfikacji oraz, jakie mają czy też mogą być, ich skutki. Nie została dostatecznie przemyślana cała koncepcja ustawy nowelizacyjnej i aktualnie ponownie należałoby powrócić do ustalenia samej strategii nowelizacji i jej celu. Zmiany w UKSC należałoby oprzeć na równowadze wartości społecznych i gospodarczych, a chociażby na poszanowaniu obu grup wartości i ich

wyważeniu. Koncepcja, która zdaje się leżeć u podstaw Projektu, nie jest oparta na takich założeniach, co KIKE szczegółowo zaprezentuje poniżej w niniejszym piśmie.

2. Niedostateczne uzasadnienie Projektu, naruszenie art. 66 ustawy Prawo przedsiębiorców

Uzasadnienie Projektu nie spełnia wymogów ustanowionych w art. 66 ust. 1 *ustawy Prawo przedsiębiorców* (zwanej dalej **UstPP**), zgodnie z którym:

> *Przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania, wykonywania lub zakończenia działalności gospodarczej dokonuje się:*
>
> *a) analizy możliwości osiągnięcia celu tego aktu normatywnego za pomocą innych środków;*
>
> *b) oceny przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami ustawy.*

Ani w uzasadnieniu do Projektu, ani w Ocenie Skutków Regulacji (**OSR**), nie przedstawiono twierdzeń, z których można by wywieźć, że przed przystąpieniem do prac nad zmianą przepisów UKSC, a tym bardziej nad zmianą Poprzedniego Projektu, została przeprowadza jakakolwiek analiza możliwości skorzystania z innych, niż wskazane w Projekcie, metod osiągniecia postawionego celu (zwiększenia bezpieczeństwa informacji). Tym bardziej, nie przedstawiono dowodów podjęcia takiej analizy czy jej efektów, które mogłyby przemawiać za ingerencją w przepisy UKSC czy w treść Poprzedniego Projektu. Nie przeprowadzono wymaganego przepisami UstPP testu proporcjonalności – oceny wpływu nowych przepisów na stosunki społeczno-gospodarcze.

Powyższe stanowi oczywisty przejaw naruszenia zasady minimalnej interwencji legislacyjnej w wolność gospodarczą, zapisanej w zacytowanym powyżej art. 66 ustawy Prawo przedsiębiorców. Jak wskazuje się w literaturze (M. Zdyb, G. Lubeńczuk, A. Wołoszyn-Cichocka, *Prawo przedsiębiorców. Komentarz*, Warszawa 2019):

> *[…] obowiązek ten* [tj. obowiązek uregulowany w art. 66] *rodzi konieczność rozważenia możliwości osiągnięcia określonych celów za pomocą innych środków, w tym w szczególności możliwości powstrzymania się w danym przypadku od ingerencji prawnej, zgodnie z regułą, że interwencja legislacyjna stanowi ostateczność. Mając na względzie fakt, że ustawodawca wiąże wskazany obowiązek z dyrektywą wynikającą z art. 22 Konstytucji RP, kryterium oceny dopuszczalności zastosowania określonych rozwiązań, powinien być wynikający z tego przepisu wymóg uzasadnienia ingerencji w sferę wolności działalności gospodarczej ważnym interesem publicznym. […] Artykuł 66 ust. 2 PrPrzed wprowadza obowiązek zamieszczenia wyników oceny i analiz, o których mowa w art. 66 ust. 1 PrPrzed, w uzasadnieniu do projektu aktu normatywnego lub w ocenie skutków regulacji, stanowiącej odrębną część uzasadnienia projektu aktu normatywnego.*

Pomimo przywoływanych przez stronę społeczną wyliczeń i wyników analiz, które niekorzystnie odnoszą się do podjętej inicjatywy ustawodawczej, załączona do projektu OSR nie odnosi się do podniesionych okoliczności w żadnym zakresie. Nawet jeżeli projektodawca nie chciał skorzystać z informacji przekazanych przez stronę społeczną, to w okresie od zakończenia etapu konsultacji publicznych do dnia publikacji nowej wersji projektu, projektodawca mógł przeprowadzić samodzielnie taką ocenę lub skorzystać ww. zakresie z pomocy odpowiednich ośrodków naukowych i badawczych. Otrzymane wyniki zapewne potwierdziłby te argumenty, które przedstawiła strona społeczna, a przede wszystkim umożliwiłyby rzeczowe odniesienie się do tych argumentów, w tym zweryfikowanie ich zasadności.

Z uwagi na to, że doszło do naruszenia art. 66 ust. 2 UstPP, aktualnie nie wiadomo, czy przed wprowadzeniem zmian do Projektu, a nawet do samej UKSC, rozważono inne, mniej uciążliwe i przede

wszystkim w pełni zgodne z ustawą zasadniczą, sposoby zwiększenia bezpieczeństwa informacji (cyberbezpieczeństwa).

KIKE podkreśla przede wszystkim, że w **OSR nie odniesiono się do potencjalnych kosztów wprowadzenia rozwiązań przewidzianych w Projekcie**, w szczególności w zakresie obowiązków wycofania sprzętu telekomunikacyjnego danych dostawców, a w zasadzie całkowitego wykluczenia konkretnych dostawców sprzętu/oprogramowania. Zasadniczy problem, opisany m.in. w stanowisku KIKE, wyrażonym odnośnie do Poprzedniego Projektu, nadal nie został rozwiązany, co zostanie niżej przedstawione. Tymczasem, decyzje o uznaniu dostawców za dostawców wysokiego ryzyka, mogą skutkować daleko idącymi, negatywnymi skutkami społecznymi (takimi jak likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego, utrata zaufania do działań organów publicznych czy co do pewności praw i obowiązków wyrażonych w przepisach prawa, nasilenie postaw skrajnie nacjonalistycznych czy ksenofobicznych) oraz gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów, uprzywilejowanie części dostawców, ograniczenie konkurencji i wprowadzenie monopoli wspieranych przez organy administracji publicznej).

W OSR wskazano tylko, że nie można dokonać obliczeń/szacunków kosztów wdrożenia rozwiązań przewidzianych w Projekcie, pomimo że w ramach konsultacji publicznych zostały przedłożone raporty dotyczące wpływu poszczególnych instytucji uregulowanych w Projekcie na rynek telekomunikacyjny. Analiza skutków finansowych wprowadzonych regulacji ogranicza się do analizy kosztów związanych z działalnością administracji państwowej, wygenerowanych z tytułu nowych regulacji. Tymczasem, powinny zostać przede wszystkim wyliczone/oszacowane te konsekwencje finansowe, które dotyczą prawdopodobnego wzrostu cen usług telekomunikacyjnych (co odczuje całe społeczeństwo, w tym konsumenci oraz przewidywanego wzrostu kosztów działalności dla operatorów telekomunikacyjnych - albowiem tylko wtedy można będzie dokonać prawidłowej i wyczerpującej oceny skutków finansowych wprowadzonych ograniczeń. Społeczeństwo (w szczególności konsumenci i przedsiębiorcy, w tym operatorzy telekomunikacyjni) powinni wiedzieć, jakie będą dla nich skutki finansowe i gospodarcze proponowanych regulacji prawnych.

W uzasadnieniu Projektu oraz OSR nie podjęto również analizy skutków projektowanej regulacji w stosunku do zobowiązań Rzeczpospolitej Polskiej wynikających z przepisów prawa międzynarodowego. Nie rozważano także tego, jaki będzie wpływ Projektu na wdrożenie sieci 5G w Polsce, w szczególności tego, czy rozwiązania przewidziane w Projekcie nie opóźnią rozwoju sieci 5G w Polsce.

UWAGI SZCZEGÓŁOWE

Niżej przedstawiono spostrzeżenia do Projektu w czterech kategoriach – w formie uwag do: **(1)** koncepcji operatora sieci komunikacji strategicznej; **(2)** procedury postępowania w sprawie uznania za dostawcę wysokiego ryzyka; **(3)** procedur wydawania ostrzeżeń oraz poleceń zabezpieczających; **(4)** zmian w UstPT.

1. Koncepcja operatora sieci komunikacji strategicznej

Projekt w rozdziale 11b przewiduje utworzenie sieci komunikacji strategicznej oraz powołanie do pełnienia funkcji operatora tej sieci jednoosobowej spółki Skarbu Państwa. KIKE nie zgadza się z twierdzeniem zawartych w uzasadnieniu Projektu, jakoby w obecnym stanie prawnym brak było podobnych rozwiązań. Koncepcja ta nawiązuje bowiem do idei OSE oraz powołania NASK-u na operatora tej sieci. Już z tej przyczyny KIKE wnosi o reasumpcję tego pomysłu, albowiem jak powszechnie wiadomo, prawidłowość, a przede wszystkim efektywność funkcjonowania NASK bywała w przeszłości różnie oceniana. Wielokrotnie zdarzało się, że instytucja ta nie była przygotowana do funkcji, jaką miała pełnić lub też nie do końca była w stanie sprostać stawianym jej zadaniom.

KIKE zwraca także uwagę na kolizję projektowanej instytucji z projektem ustawy o Sieci Łączności Rządowej (projekt Ministra Spraw Wewnętrznych i Administracji z dnia 21 maja 2019 r., numer z wykazu UD333). W ocenie KIKE, ewentualne koncepcja operatora sieci komunikacji strategicznej, czy też samej sieci komunikacji strategicznej, powinna zostać uregulowana właśnie we wspomnianym projekcie, gdzie zajęłaby miejsce pierwszorzędne i gdzie można by poświęcić jej w całym procesie legislacyjnym dostateczną ilość uwagi. Nie jest zaś właściwym miejscem na regulowanie omawianej kwestii UKSC. Zakres tematyczny projektowanych regulacji wykracza poza ramy przedmiotowe UKSC.

Na podstawie lektury art. 59zd ust. 1 oraz jego uzasadnienia, można by stwierdzić, iż z Projektu wynika, że sieć komunikacji strategicznej ma być budowana w całości od podstaw, albowiem ma się cechować innym poziomem bezpieczeństwa informacji niż sieci innych przedsiębiorców – a zatem *de facto* tą siecią nie powinny być sieci (lub ich elementy), wykorzystywane w innym celu niż określony w art. 59zd ust. 1 oraz posiadane przez innych przedsiębiorców niż operator sieci komunikacji strategicznej. Takie założenie byłoby jednak sprzeczne z zasadami wyrażonymi w polskich i unijnych aktach prawnych, które nakazują unikania dublowania istniejących sieci telekomunikacyjnych i forsują ideę współkorzystania z sieci.

Tymczasem, z art. 59zd ust. 2 wprost wynika, że operatorem sieci komunikacji strategicznej ma być spółka **posiadająca infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w art. 59zd ust. 1** – co może sugerować, że operatorem tym może być jedynie ta spółka, która będzie właścicielem infrastruktury wymaganej do realizacji wspomnianych zadań lub też, która będzie się względem tej infrastruktury zachowywać jak właściciel. Większość usług hurtowego dostępu do sieci nie przyznaje zaś operatorowi korzystającemu tak szerokich uprawnień względem sieci/infrastruktury operatora sieci dostępowej, jaki ma właściciel sieci.

Z art. 59zf wynika, że operator sieci komunikacji strategicznej może jednak na potrzeby komunikacji strategicznej korzystać z sieci telekomunikacyjnych innych operatorów – co nie wydaje się spójne z wyżej opisanymi przepisami, odnoszącymi się do instytucji operatora sieci komunikacji strategicznej. Projekt nie wyjaśnia, czy w sytuacji udostępnienia sieci operatorowi komunikacji strategicznej przez innego przedsiębiorcę, sieć ta - w zakresie objętym dostępem - staje się częścią sieci komunikacji strategicznej, o której mowa w art. 59zd ust. 1 lub też, czy takie udostępnienie skutkuje wyłączeniem obowiązku/możliwości innego wykorzystania tej sieci, w tym w celu świadczenia usług telekomunikacyjnych detalicznych lub hurtowych przez właściciela sieci. Projekt powinien wyraźnie odpowiadać na te wątpliwości. Jakkolwiek, KIKE sygnalizuje, że nie sposób zrozumieć:

- w jakim celu miałoby dojść do stworzenia z elementów sieci innych przedsiębiorców, sztucznego tworu w postaci sieci komunikacji strategicznej na potrzeby komunikacji strategicznej;
- w jakim celu mówi się o sieci komunikacji strategicznej, jeśli operator sieci komunikacji strategicznej miałby *de facto* świadczyć usługi telekomunikacyjne w oparciu o usługi hurtowego dostępu do sieci innych przedsiębiorców telekomunikacyjnych.

Art. 59zf ust. 1 stanowi o tym, że każdy z operatorów telekomunikacyjnych jest zobowiązany zapewnić odpłatnie dostęp do elementów sieci telekomunikacyjnej na potrzeby komunikacji strategicznej realizowanej przez operatora sieci komunikacji strategicznej. Jednocześnie, z art. 1 ust. 2 pkt 1 UKSC z uwzględnieniem zmian zapisanych w Projekcie, wynika, że art. 59zf nie ma zastosowania do przedsiębiorców telekomunikacyjnych. Wyjaśnienia zatem wymaga, jaki jest cel regulacji zawartej w analizowanym art. 59zf, skoro wyłączono jej obowiązywanie wobec przedsiębiorców telekomunikacyjnych. Oba wskazane przepisy są ze sobą wyraźnie sprzeczne.

Odnosząc się zaś do samego obowiązku zapewnienia dostępu hurtowego do sieci przez innych operatorów telekomunikacyjnych na rzecz operatora sieci komunikacji strategicznej, KIKE sprzeciwia się temu, aby

wprowadzone zostały w tym zakresie zasady uprzywilejowujące operatora sieci komunikacji strategicznej wobec innych przedsiębiorców telekomunikacyjnych. Tymczasem, takie właśnie uregulowanie tych kwestii proponuje się w Projekcie. W Projekcie modyfikuje się powszechnie obowiązujące zasady udostępniania sieci telekomunikacyjnych, w szczególności wynikające z UstPT oraz *ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych* - na korzyść operatora sieci komunikacji strategicznej. Wyrazem tego jest zapisanie w projektowanym art. 59zf ust. 3 UKSC tego, że operator sieci komunikacji strategicznej może zwrócić się do Prezesa UKE o wydanie decyzji w sprawie dostępu do sieci już po upływie 30 dni od złożenia wniosku o dostęp (o ile nie dojdzie do zawarcia umowy o dostępie).

KIKE uważa, iż w UKSC nie powinno się zmieniać zasad dostępu hurtowego do sieci telekomunikacyjnych, uregulowanych w innych, właściwych przepisach. Ponadto, należałoby rozważyć, czy wprowadzenie ewentualnych modyfikacji zasad powszechnie obowiązujących w tym zakresie, nie wymaga uzyskania stanowiska/zgody Komisji Europejskiej w zakresie zgodności takiego mechanizmu z prawem unijnym.

Gdyby koncepcja operatora sieci komunikacji strategicznej miała się ostać w Projekcie – czemu KIKE się sprzeciwia - KIKE apeluje o:

- doprecyzowanie w treści przepisu art. 59zd ust. 5 przypadków, w których operator sieci komunikacji strategicznej będzie mógł – za zgodą Prezesa Rady Ministrów – świadczyć usługi telekomunikacyjne także podmiotom innym niż wskazane w art. 59zd ust. 4;
- **wyraźne wskazanie w Projekcie, czy operator sieci komunikacji strategicznej będzie miał monopol na świadczenie usług telekomunikacyjnych na rzecz podmiotów określonych w art. 59zd ust. 4. Innymi słowy, czy po wejściu w życie opisywanych zmian na rzecz tych podmiotów, będzie dozwolone świadczenie usług telekomunikacyjnych przez przedsiębiorców telekomunikacyjnych innych niż operator sieci komunikacji strategicznej.**

2. Procedura postępowania w sprawie uznania za dostawcę wysokiego ryzyka

2.1. Przedmiot postępowania

Aktualne rozwiązanie: postępowanie odnosi się do dostawcy, z którego produktów, usług lub procesów korzystają podmioty wymienione w Projekcie

Proponowane rozwiązanie: postępowanie powinno odnosić się konkretnych produktów, usług i procesów (a nie do ich dostawcy) i to jedynie **do produktów, usług lub procesów krytycznych dla bezpieczeństwa sieci i usług**, z których korzystają podmioty wymienione w ustawie

Projekt niestety w dalszym ciągu zawiera rozwiązanie, że postępowanie w sprawie uznania za dostawcę wysokiego ryzyka (dalej **Postępowanie**) ma się toczyć w sprawie uznania danego podmiotu za dostawcę wysokiego ryzyka, a nie w przedmiocie zakwalifikowania konkretnego sprzętu/oprogramowania, jako stwarzającego wysokie ryzyko.

Takie podejście do tego zagadnienia należy uznać za nieprawidłowe, albowiem może skutkować napiętnowaniem danego przedsiębiorcy, negatywnym oddziaływaniem na całą markę/wizerunek tego przedsiębiorcy. Proponowana regulacja nie odzwierciedla też celu, jakiemu mają służyć nowe przepisy, identyfikowanemu – przynajmniej w ocenie KIKE - jako wyeliminowanie z użytku sprzętu/oprogramowania, który będzie stwarzał duże prawdopodobieństwo wystąpienia niepożądanego zdarzenia. Procedura opisana w Projekcie zdaje się prowadzić nie do tego, aby wykluczyć pewny, konkretny rodzaj sprzętu/oprogramowania z użytku, a do tego, aby wyprzeć danego dostawcę z całego kraju, czy dostawców pochodzących z określonych obszarów/kraju. Nie jest też tajemnicą, z jakiego sprzętu korzystają operatorzy zrzeszeni w KIKE, co pokazały wyniki badań przeprowadzone przez Izbę przy

okazji konsultacji Poprzedniego Projektu. I to nie tylko dostawca/producent takiego sprzętu odczuje skutki regulacji, ale korzystający z niego operatorzy, a w ostatecznym rozrachunku konsumenci.

Aktualna koncepcja prowadzenia Postępowania co do określonego dostawcy może mieć taki skutek, że całkowicie uniemożliwi danemu przedsiębiorstwu funkcjonowanie w Polsce, w tym uczyni nieopłacalnym prowadzenie przez niego działalności gospodarczej w jakimkolwiek przedmiocie (nie tylko co do sprzętu czy oprogramowania, które można by zakwestionować z uwagi na przesłankę bezpieczeństwa). W przypadku uznania danego podmiotu za dostawcę wysokiego ryzyka, firma tego przedsiębiorcy będzie bowiem identyfikowana z wysokim ryzykiem czy zagrożeniem bezpieczeństwa (będzie wzbudzała negatywne emocje), a tym samym oferowane przez tego przedsiębiorcę towary czy usługi (choćby dotyczące innego profilu działalności) nie będą wzbudzały zaufania i nie będzie na nie popytu.

Powyższe potwierdzają kryteria (w większości niezmienione względem Poprzedniego Projektu), które ma wziąć pod uwagę Kolegium przy sporządzaniu opinii w zakresie uznania dostawcy za dostawcę wysokiego ryzyka. Zgodnie z art. 66a ust. 6, opinia Kolegium ma zawierać analizę m.in.:

> *prawdopodobieństwa, z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:*
>
> *a) stopnia i rodzaju powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,*
>
> *b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,*
>
> *c) struktury własnościowej dostawcy sprzętu lub oprogramowania,*
>
> *d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania*

- oraz m.in.:

> *trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt. 1-4, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania* i *treści wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.*

Są to kryteria, które nie zostały usunięte z Poprzedniego Projektu i KIKE podtrzymuje, że są one subiektywne, upolitycznione, niejasne, nieprzejrzyste, uznaniowe i istnieje wątpliwość w jaki sposób Kolegium ma w ogóle ocenić ich spełnienie. Kryteria te nie mają wpływu na bezpieczeństwo samego sprzętu czy oprogramowania - a zatem kategorycznie powinny zostać z Projektu usunięte. Na podstawie tak sformułowanych kryteriów, Kolegium musiałoby poddać wnikliwej analizie cały system prawny danego państwa, weryfikować występowanie zjawiska nepotyzmu czy sposób, w jaki przebiega proces produkcyjny. Projekt obecnie nakazuje Kolegium analizę struktury własnościowej dostawcy – nie wiadomo zaś, jak daleko Kolegium ma się zagłębiać w tą kwestię. W szczególności, nie sposób ustalić, czy ustawodawca oczekuje jedynie ustalenia danych wspólników bądź akcjonariuszy dostawcy (i to jakich konkretnie danych), czy też wymaga od Kolegium dalszej analizy pochodzenia, pokrewieństwa bądź jeszcze innych zagadnień dotyczących wspólników bądź akcjonariuszy.

Co więcej, Kolegium nie będzie zobowiązane wykazać, iż dane państwo faktycznie jest zdolne ingerować w swobodę działalności danego dostawcy i czy rzeczywiście występują powiązania dostawcy z władzami danego państwa, a wystarczające będzie tylko uprawdopodobnienie, iż taka ingerencja jest możliwa. W Projekcie bowiem mowa jest o prawdopodobieństwie, które to słowo należy rozumieć jako *możliwość,*

szansę wydarzenia się czegoś[1]. Kolegium ma zatem jedynie prognozować, szacować poszczególne okoliczności, zaś dostawca będzie ponosił wysoce uciążliwe konsekwencje tych szacunków czy prognoz. Kolegium ma oceniać możliwość/prawdopodobieństwo stopnia możliwego/prawdopodobnego wpływu państwa trzeciego na działalność danego przedsiębiorstwa. Opinia Kolegium ma się zatem sprowadzać do podejrzeń, hipotez, przewidywań, wróżb i prognoz – a zatem do działań nieudowodnionych, a jedynie w jakimś stopniu subiektywnie podejrzewanych/przewidywanych przez członków Kolegium.

Wysoce wątpliwa jest możliwość jakiejkolwiek weryfikacji opinii, albowiem nie sposób określić, w jaki sposób konkretny przedsiębiorca, zainteresowany wynikiem postępowania, miałby korespondować z subiektywnymi przewidywaniami danego członka Kolegium. Nie zostały bowiem sformułowane żadne wymogi, standardy czy wytyczne, które opinia Kolegium ma spełniać. Opisywany problem można swobodnie porównać do prognozy pogody, która choć zwykle opiera się na monitorowaniu zbliżonych bądź tożsamych czynników, to jej treść jest zależna od tego, przez kogo została sformułowana.

Z uwagi na daleko idące konsekwencje uznania dostawcy za stwarzającego niebezpieczeństwo, stwierdzić należy, że wydanie opinii oceniającej dostawcę negatywnie w oparciu nie o fakty (i to fakty udowodnione), a uprawdopodobnienia/oceny czy szacunki – jest w demokratycznym państwa prawa, jakim jest Rzeczpospolita Polska, całkowicie niedopuszczalne.

Nie sposób również pominąć tego, że omawiane kryteria są tak sformułowane, że w zasadzie dyskryminują danego przedsiębiorcę z uwagi na miejsce siedziby/miejsce pochodzenia wspólników/akcjonariuszy, panujący w tym kraju ustrój polityczny, treść ustawodawstwa i tym podobne okoliczności, na które przedsiębiorca ten nie ma żadnego wpływu.

Zdaniem KIKE, takie podejście legislacyjne ma przede wszystkim uderzać w dostawców sprzętu/oprogramowania pochodzącego z Azji. Faktem powszechnie znanym jest zaś to, że praktycznie zdecydowana większość sprzętu użytkowanego przez przedsiębiorców telekomunikacyjnych w Polsce jest dostarczana właśnie przez dostawców z tych terenów. Wynika to z tego, że sprzęt/oprogramowanie europejskie jest droższe, co wcale nie przekłada się na lepszą jakość czy większe bezpieczeństwo. Wyeliminowanie z użytku sprzętu tego pochodzenia wymusi zatem na operatorach zakup droższego, lecz wcale nie lepszego czy bezpieczniejszego sprzętu – co nie tylko przełoży się na wzrost cen za usługi świadczone na rzecz użytkowników końcowych, ale i obniży standardy bezpieczeństwa i jakość usług.

KIKE nadmienia, że **odpowiednia procedura badania urządzenia informatycznego lub oprogramowania** w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, **jest już przewidziana w art. 33 UKSC**. Zasadne zatem byłoby rozszerzenie istniejącej procedury nastawionej na zapewnienie bezpieczeństwa sprzętu i oprogramowania (i badanie konkretnego sprzętu/oprogramowania) - co jest celowe z punktu widzenia bezpieczeństwa informacji - zamiast tworzenia zupełnie nowej procedury, mającej z założenia rzekomo spełniać tożsame funkcje, a nastawionej na kryterium podmiotowe i stygmatyzowanie całego przedsiębiorstwa. Aktualnie w Projekcie proponuje się uznanie dostawcy (czyli całego przedsiębiorcy/całej marki) za stwarzającego zagrożenie dla bezpieczeństwa narodowego, a nie z uznanie konkretnego sprzętu/oprogramowania za niedostatecznie zapewniającego bezpieczeństwo, czy generującego pewne ryzyko.

Nie można przy tej okazji zapominać, że przewidziane w Projekcie rozwiązania „stygmatyzacji" wcale nie zmierzają do wyeliminowania ryzyka zajścia incydentów w zakresie cyberbezpieczeństwa, a wręcz

[1] https://sjp.pwn.pl/sjp/prawdopodobienstwo;2507927.html [dostęp w dniu 03.02.2021 r.]

przeciwnie, doprowadzą do tego, że ryzyk tych będzie więcej. Rynek nie znosi próżni, operatorzy poszukiwać będą tańszych rozwiązań, wyeliminowanie wskazanego z „imienia i nazwiska" dostawcy spowoduje najpewniej, że tak powstała luka będzie zapełniona sprzętem anonimowych dostawców, nie objętych decyzją Ministra, którzy niekoniecznie muszą dbać o renomę i jakość oferowanego sprzętu, w tym jego należyty serwis czy update oprogramowania. Nie trzeba zapewne rozwijać myśli, w jaki sposób wpłynie to na kwestie cyberbezpieczeństwa w polskich sieciach telekomunikacyjnych i ryzyko zajścia krytycznych incydentów.

2.2. Przesłanki wydania decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka oraz kryteria oceny ich wystąpienia

Aktualne rozwiązanie: przesłanki wydania decyzji uznającej przedsiębiorcę za dostawcę wysokiego ryzyka oraz kryteria oceny ich spełnienia (w szczególności te, które ma rozważyć Kolegium w wydawanej opinii) są subiektywne i odnoszą się przede wszystkim do oceny przedsiębiorcy i możliwości wywierania wpływu na niego przez państwo trzecie

Proponowane rozwiązanie: przesłanki wydania decyzji uznającej przedsiębiorcę za dostawcę wysokiego ryzyka oraz kryteria oceny ich spełnienia (w szczególności te, które ma rozważyć Kolegium w wydawanej opinii) powinny w najszerszym możliwym stopniu mieć charakter techniczny, a ich weryfikacja powinna się opierać na obiektywnym badaniu (pomiarze)

Zgodnie z wyżej przywołanym projektowanym art. 66a ust. 8, decyzja ma zostać wydana, jeżeli **z przeprowadzonego postępowania wynika**, że dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla bezpieczeństwa narodowego.

Powstaje zatem pytanie – co powoduje, że dostawca sprzętu lub oprogramowania stwarza zagrożenie dla bezpieczeństwa narodowego i to poważne zagrożenie? Decyzja jest wydawana przez ministra właściwego do spraw informatyzacji. Minister ten - przed rozstrzygnięciem sprawy – zasięga opinii Kolegium, jeśli Postępowanie wszczęto z urzędu. W przypadku Postępowania wszczętego na wniosek, opinia Kolegium jest zawarta we wniosku. W zakresie specjalistycznego materiału dowodowego gromadzonego w Postępowaniu (abstrahując od postanowień Kodeksu postępowania administracyjnego określających ogólne zasady prowadzenia postępowania dowodowego w każdym postępowaniu administracyjnym) w Projekcie przewidziano jedynie opinię Kolegium.

KIKE ponownie podnosi problem braku przewidzianego obowiązku uwzględnienia kryteriów technicznych ocenianego sprzętu lub oprogramowania. Zupełnie niezrozumiałym jest, dlaczego nie jest przewidziany obowiązek przeprowadzenia np. testów penetracyjnych sprzętu lub oprogramowania, jako miarodajniejszych i obiektywnych kryteriów oceny, niż obecnie przewidziane w Projekcie kryteria.

Wbrew uzasadnieniu do Projektu, kryteria oceny o charakterze technicznym (art. 66a ust. 6 pkt 4-6 UKSC w brzmieniu zaprezentowanym w Projekcie) są niezwykle ograniczone i takiego rodzaju, że nie będą w praktyce odgrywać decydującej roli. Stwarza to ciągle niebezpieczeństwo uznaniowości oceny, zwłaszcza przy równoczesnym utajnieniu prac i dostępu do ich wyników oraz ograniczeniu możliwości wnoszenia środków zaskarżenia (o czym szerzej w dalszej części niniejszego stanowiska).

W uzasadnieniu do Projektu czytamy:

> *nie jest możliwe ograniczenie się w analizie dostawcy sprzętu lub oprogramowania wyłącznie do aspektów technicznych oferowanych przez niego produktów ICT, usług ICT czy procesów ICT. Postęp technologiczny nie tylko zapewnił poprawę jakości komunikacji ale także umożliwił nowe formy*

ingerencji państw trzecich w bezpieczeństwo narodowe. Coraz więcej urządzeń jest stale podłączonych do globalnej sieci, co powoduje że w każdej chwili jest przesyłana ogromna ilość danych. Dla służb wywiadowczych obcych państw są to potencjalnie potężne zasoby informacyjne, które mogą zostać wykorzystane przeciwko Polsce. Ponadto dostęp do urządzeń stale podłączonych do sieci poprzez ukryte (lub celowo zaprojektowane) podatności mógłby skutkować przejęciem kontroli nad znaczną liczbą urządzeń używanych przez podmioty krajowego systemu cyberbezpieczeństwa, czy operatorów infrastruktury krytycznej

– **stanowisko takie zawiera błąd logiczny i jest wewnętrznie sprzeczne**. Z jednej strony projektodawca wskazuje, że nie jest możliwe ograniczenie się wyłącznie do aspektów technicznych, a z drugiej wskazuje, że dostęp do urządzeń mógłby nastąpić przez celowo wprowadzone podatności sprzętu/oprogramowania. **Istnienie podatności możliwe jest do zweryfikowania wyłącznie poprzez zbadanie sprzętu**. Innymi słowy, takiej podatności nie stwierdzi Kolegium, analizując strukturę własnościową dostawcy. Inną kwestią jest to, że jeśli sprzęt nie jest bezpieczny, tj. zawiera podatności, to hipotetycznie każdy ma możliwość uzyskania dostępu do danych – nie tylko służby wywiadowcze państwa trzeciego, ale również i cyberprzestępcy.

Ani żadne państwo trzecie, ani służby wywiadowcze, ani przestępcy nie uzyskają dostępu do danych, jeśli sprzęt i sieć są odpowiednio zabezpieczone. Z tego względu aspekty techniczne powinny być decydującym czynnikiem w Postępowaniu, a ewentualne kryteria dot. systemu prawnego czy powiązań z władzami państwa trzeciego, powinny być brane ewentualnie pod uwagę i tylko pomocniczo. Celem procedury nie jest przecież uniemożliwienie dostępu do danych wyłącznie służbom państw trzecich, ale uniemożliwienie dostępu do danych jakiemukolwiek nieuprawnionemu podmiotowi.

Reasumując, KIKE podnosi, że obecna treść Projektu sugeruje, że kluczowym dowodem jaki minister ma wziąć pod uwagę, jest opinia Kolegium, podczas gdy decydującym dowodem powinien być wynik weryfikowalnych i jednoznacznych badań oraz wykrytych w wyniku tych badań podatności danego sprzętu lub oprogramowania - szczególnie, że przeprowadzenie takiego dowodu w Postępowaniu nie jest niedopuszczalne z punktu widzenia przepisów ustawy Kodeks postępowania administracyjnego (zwanej dalej **KPA**). Zgodnie z art. 75 § 1 KPA:

Jako dowód należy dopuścić wszystko, co może przyczynić się do wyjaśnienia sprawy, a nie jest sprzeczne z prawem. W szczególności dowodem mogą być dokumenty, zeznania świadków, opinie biegłych oraz oględziny.

Kluczową kwestią w Postępowaniu powinno być uzyskanie odpowiedzi na następujące pytanie: czy można przełamać zabezpieczenia danego sprzętu/oprogramowania, a jeśli tak – jak trudne jest przełamanie tych zabezpieczeń? **Odpowiedź na tak postawione pytanie można uzyskać wyłącznie poprzez zbadanie i przetestowanie danego sprzętu czy oprogramowania, a nie poprzez przeanalizowanie systemu prawnego państwa, z którego dostawca tego sprzętu/oprogramowania pochodzi.** Oparcie decyzji wydawanej w Postępowaniu na kryteriach nietechnicznych jest rozwiązaniem absurdalnym, kompletnie oderwanym od celu regulacji, jakim jest zapewnienie cyberbezpieczeństwa na poziomie krajowym (art. 3 UKSC). Projektodawca pośrednio to przyznaje w zacytowanym wyżej fragmencie uzasadnienia do Projektu – co tym bardziej potwierdza zasadność powyższego stanowiska KIKE.

2.3. Przesłanka bezpieczeństwa narodowego

Aktualne rozwiązanie:	dostawca stanowi poważne zagrożenie dla bezpieczeństwa narodowego
Proponowane rozwiązanie:	produkty, usługi lub procesy oferowane przez dostawcę stanowią poważne zagrożenie dla cyberbezpieczeństwa Rzeczpospolitej Polskiej

Zgodnie z wyżej przywołanym projektowanym art. 66a ust. 8, decyzja uznająca dostawcę za dostawcę wysokiego ryzyka, ma zostać wydana, **jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego.** KIKE uważa, że decyzja powinna dotyczyć uznania konkretnego sprzętu/oprogramowania za sprzęt/oprogramowanie stanowiące poważne zagrożenie dla cyberbezpieczeństwa Rzeczpospolitej Polskiej.

Ponadto, nie sposób pominąć tego, że kluczowe dla rozstrzygnięcia postępowania określenia *bezpieczeństwa narodowego* oraz *poważnego zagrożenia* nie posiadają definicji legalnych, w szczególności takich definicji nie zawiera UKSC i nie zostały ona przedstawione w treści Projektu. W uzasadnieniu do Projektu (s. 82), projektodawcy powołują się na poglądy doktryny odnośnie do definicji *bezpieczeństwa narodowego* wskazując, że pojęcie to rozumiane jest jako:

> *kategoria obejmująca bezpieczeństwo państwa, bezpieczeństwo obywateli, bezpieczeństwo wewnętrzne, bezpieczeństwo zewnętrzne, oraz porządek publiczny.*

Poglądy doktryny nie są jednak jednolite i w polskim systemie prawnym nie mogą one stanowić źródła prawa, zwłaszcza w kwestii tak newralgicznej, która może decydować o losach dużych przedsiębiorstw, a pośrednio szeregu małych i średnich firm. Brak zdefiniowania omawianych pojęć może mieć wysoce negatywne skutki. Przede wszystkim zagadnienie to będzie rodzić liczne wątpliwości interpretacyjne dotyczące określenia, czym jest bezpieczeństwo narodowe i kiedy zachodzi jego poważnie zagrożone. Pozostawia to nadmiernie szeroki luz decyzyjny dla ministra, który będzie mógł uznaniowo uznawać, że została spełniona przesłanka poważnego zagrożenia dla bezpieczeństwa narodowego. Nie sposób również wykluczyć tego, że z biegiem czasu dojdzie na tle omawianej wykładni do rozbieżności w orzecznictwie, co z punktu widzenia zasady pogłębiania zaufania uczestników postępowania do władzy publicznej, zapisanej w art. 8 KPA, jest niepożądane.

W ocenie KIKE, zamiast przesłanki poważnego zagrożenia bezpieczeństwa narodowego w art. 66a ust. 8 należy wprowadzić przesłankę *zagrożenia cyberbezpieczeństwa*. Zarówno bowiem pojęcie *zagrożenia*, jak i pojęcie *cyberbezpieczeństwa* doczekały się swoich definicji legalnych na gruncie UKSC**.**

2.4. Indywidualny charakter decyzji administracyjnej a skutki wobec podmiotów trzecich

Rozwiązanie Projektu: decyzja adresowana do dostawcy wywiera skutek wobec podmiotów trzecich, które nie są uczestnikami postępowania

Projekt przewiduje, że uznanie dostawcy za dostawcę wysokiego ryzyka następuje w drodze decyzji administracyjnej, zaś wydanie takiej decyzji wobec dostawcy ma wywierać określone skutki wobec podmiotów trzecich. Zgodnie z projektowanym art. 66b ust. 1 i 2, w przypadku wydania decyzji uznania za dostawcę wysokiego ryzyka, określone podmioty (inne niż adresat decyzji) będą mieć: (1) zakaz wprowadzania do użytkowania produktów ICT, rodzajów usług ICT i konkretnych procesów w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka oraz (2) nakaz wycofania z użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat (a właściwie 5 lat) od dnia opublikowania informacji o decyzji. Szczegółowe uwagi dotyczące iluzoryczności 7-letniego terminu na wycofanie sprzętu zostaną przedstawione w dalszej części niniejszego stanowiska.

Powyższe oznacza, że decyzja nie ma mieć charakteru indywidualnego, skoro zasadniczo będzie wywierać skutki wobec osób trzecich, które to osoby nie będą mieć możliwości udziału w takim postępowaniu, a które będą mieć interes w wydaniu decyzji o określonej treści.

Takie rozwiązanie nie jest znane w polskim systemie prawnym i nie jest dopuszczalne w świetle przepisów KPA. Zgodnie z doktryną prawa administracyjnego, decyzja administracyjna ma charakter indywidualny –

jest skierowana do oznaczonego indywidualnie adresata i kształtuje (konkretyzuje) jego prawa i obowiązki. Oznaczenie stron lub strony decyzji wskazuje na podmioty praw lub obowiązków, a więc te, które z decyzji nabyły prawa lub dla których ona ich nie tworzy. Naczelny Sąd Administracyjny w wyroku z dnia 22 września 1983 r. w sprawie o sygnaturze akt SA/Wr 367/83 wskazał:

> *decyzją administracyjną jest jednostronne rozstrzygnięcie organu administracji państwowej o wiążących konsekwencjach obowiązującej normy prawnej dla indywidualnie określonego podmiotu i konkretnej sprawy, podjęte przez ten organ w sferze stosunków zewnętrznych.*

Podobne stanowisko wyrażono przykładowo w wyroku WSA w Szczecinie z dnia 6 marca 2008 r. w sprawie o sygnaturze akt II SA/Sz 1193/07 i wyroku WSA w Warszawie z dnia 24 stycznia 2007 r. w sprawie o sygnaturze akt IV SA/Wa 2006/06.

KIKE zwraca uwagę, że zgodnie z 87 Konstytucji Rzeczypospolitej Polskiej:

> *1. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia.*
>
> *2. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są na obszarze działania organów, które je ustanowiły, akty prawa miejscowego.*

Projekt natomiast przewiduje jakieś hybrydowe, nieznane ustawie zasadniczej, źródło prawa – źródłem obowiązków np. dla danego przedsiębiorcy telekomunikacyjnego, ma być UKSC oraz decyzja administracyjna wydana w postępowaniu toczącym się bez udziału tego przedsiębiorcy wobec zupełnie innego podmiotu (tj. dostawcy). A zatem, teoretycznie hipotetyczny obowiązek ogólnie określony jest w ustawie (projektowany art. 66b ust. 1), jednakże treść obowiązku nie jest konkretna i nie dotyczy indywidualnego podmiotu (np. ABC sp. z o.o., a jedynie pewnych zbiorów podmiotów posiadających określone cechy, np. przedsiębiorców telekomunikacyjnych zobowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń) i obowiązek ten w zasadzie nie istnieje dopóki nie zostanie wydana decyzja administracyjna, o której mowa w art. 66a ust. 8. Wobec czego obowiązek w zasadzie powstaje (zaczyna obowiązywać w konkretnej treści i wobec konkretnego podmiotu) dopiero w drodze decyzji wskazującej sprzęt/oprogramowanie wyłączone z użytkowania. Decyzja administracyjna jest zaś wydawana w Postępowaniu, które toczy się bez udziału tego konkretnego podmiotu (np. przedsiębiorcy telekomunikacyjnego), ale wywiera wobec niego skutek na podstawie ogłoszenia (nie decyzji, a jedynie informacji zawartych w decyzji) w Dzienniku Urzędowym Monitor Polski, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej oraz na stronie internetowej urzędu obsługującego ministra. Wspomniany przedsiębiorca telekomunikacyjny nie będzie miał żadnych środków prawnych do zaskarżenia decyzji lub wyrażenia w innej formie sprzeciwu wobec nałożonych na niego obowiązków – zostanie całkowicie pozbawiony możliwości obrony swoich interesów.

Tymczasem, **ogłoszenie nie jest źródłem powszechnie obowiązującego prawa.** Nie sposób wymagać, aby przedsiębiorcy telekomunikacyjni codziennie weryfikowali wymienione powyżej kanały informacyjne, sprawdzając, czy danego dnia nie została opublikowana informacja dotycząca sprzętu/oprogramowania, którego używają w swoim przedsiębiorstwie.

Zdaniem KIKE, zgodnie z zasadami zapisanymi w ustawie zasadniczej oraz w KPA, decyzja może co najwyżej zakazywać jej adresatowi sprzedaży (dystrybucji) określonego sprzętu/oprogramowania, a nie może mieć żadnych skutków wobec podmiotów, które nie biorą udziału w Postępowaniu (w szczególności wobec przedsiębiorców telekomunikacyjnych). Aby mówić o obowiązku wycofania sprzętu przez ISP, niezbędne byłoby nałożenie tego obowiązku albo w źródle powszechnie obowiązującego prawa (np. rozporządzeniu zawierającym wykaz urządzeń/oprogramowania wyłączonych z możliwości użytkowania) albo w drodze

indywidualnej decyzji administracyjnej, zakazującej danemu ISP (np. ABC sp. z o.o.) użytkowania określonego sprzętu/oprogramowania.

2.5. Iluzoryczność 7-letniego terminu na wycofanie urządzeń/oprogramowania dostawy z użytkowania

Aktualne rozwiązanie: dwa rodzaje terminów na wycofanie sprzętu/oprogramowania z użytkowania, z czego w praktyce i tak do przedsiębiorców telekomunikacyjnych będzie miał zastosowanie termin 5-letni

Proponowane rozwiązanie: ograniczenie skutków decyzji do zakazu wprowadzania sprzętu lub oprogramowania do użytkowania bez ingerencji w sprzęt/oprogramowanie, które są już w użytkowaniu

Projekt przewiduje, iż w razie wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka:

- w art. 66b ust. 1 i 3 - m.in. przedsiębiorcy telekomunikacyjni opisani w wyżej zacytowanym art. 66a ust. 1 pkt 2 Projektu: (1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka; (2) wycofują użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia opublikowania informacji o decyzji, o której mowa w art. 66 ust. 8 z zastrzeżeniem art. 66b ust. 2; (3) jeśli stosuje się do nich ustawę – Prawo zamówień publicznych, nie dokonują zamówień sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 8;
- w art. 66b ust. 2 - przedsiębiorcy telekomunikacyjni opisani w wyżej zacytowanym art. 66a ust. 1 pkt 2 Projektu, wycofują (brak informacji czy chodzi o zaprzestanie z użytkowania czy w ogóle utylizację stanów magazynowych czy jeszcze o inaczej rozumiane wycofanie) w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3.

Odnosząc się do tej części regulacji, KIKE podnosi, że jedynie pozornie zapewniono możliwość wycofania produktów dostawcy wskazanego w decyzji w ciągu 7 lat, albowiem w praktyce wszyscy przedsiębiorcy telekomunikacyjni, opisani w wyżej zacytowanym art. 66a ust. 1 pkt 2, będą zobowiązani do wycofania produktów dostawcy wskazanego w decyzji w ciągu 5 lat. Analizując bowiem treść załącznika nr 3 przywołanego w art. 66b ust. 2, można dojść do wniosku, że praktycznie wszystkie urządzenia wykorzystywane do świadczenia usług telekomunikacyjnych w sieciach telekomunikacyjnych należą do kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług. Dobór kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług powoduje, że przedsiębiorcy telekomunikacyjni zawsze będą objęci krótszym, 5-letnim terminem. Wszystkie wymienione w załączniku kategorie funkcji krytycznych są niezbędnymi elementami sieci telekomunikacyjnej.

Szerzej o treści załącznika nr 3 do UKSC w dalszej części stanowiska. W tym miejscu należy jedynie nadmienić, że rozwiązanie to zostało skonstruowane przez osobę, która nie ma wiedzy o architekturze sieci, jej warstwach i sposobach zabezpieczania sieci. Poddaje to w wątpliwość kompetencje projektodawców do stworzenia regulacji z zakresu cyberbezpieczeństwa, który to akt prawny powinien być regulacją ściśle techniczną i jednoznaczną. Jeśli rzeczywistym zamiarem twórców Projektu było umożliwienie przedsiębiorcom telekomunikacyjnym wycofanie urządzeń w terminie 7 lat, to należałoby odpowiednio zmodyfikować treść załącznika nr 3, a w szczególności doprecyzować jego brzmienie.

Postulaty KIKE wyrażone w stanowisku przedstawionym w ramach konsultacji Poprzedniego Projektu nie zostały więc uwzględnione. Przedsiębiorców telekomunikacyjnych nadal będzie obowiązywać pierwotnie przewidywany 5-letni termin na wycofanie sprzętu/oprogramowania z użytkowania.

KIKE ponownie wskazuje na problem poniesienia kosztów związanych z ewentualną koniecznością wymiany urządzeń lub oprogramowania, które zostało legalnie nabyte. Decyzja będzie delegalizować korzystanie z legalnie nabytych urządzeń, a koszt wymiany takich urządzeń poniosą przedsiębiorcy telekomunikacyjni. Z badania przeprowadzonego na zlecenie KIKE wynika[2], że średni koszt, jaki zmuszony będzie ponieść ISP w związku z koniecznością wymiany urządzeń, wynosi blisko 3.000.000 złotych - co oznacza, że, rozkładając ten koszt na 5 lat, ISP każdego roku musiałby przeznaczyć ok. 600.000 złotych na sam tylko zakup sprzętu.

Nie sposób zaś zrozumieć, dlaczego to ISP miałby ponieść koszty takiego stanu rzeczy oraz, czy w opisywanej sytuacji ISP przysługiwałyby roszczenia odszkodowawcze wobec dostawcy sprzętu lub jakiś innych podmiotów (np. Skarbu Państwa). Jeśli wykluczyć takie roszczenia, to znamiennym pozostaje, że kosztami takich czynności będą musieli zostać obciążeni użytkownicy końcowi, co będzie miało formę drastycznej podwyżki cen świadczonych usług telekomunikacyjnych. Nie sposób również wyeliminować takiej możliwości, że - wobec konieczności poniesienia tak sporych wydatków w omawianym zakresie - wielu przedsiębiorców telekomunikacyjnych zdecyduje się na zakończenie działalności telekomunikacyjnych bądź zostanie do tego przymuszonym w związku z zaistnieniem stanu ich niewypłacalności. Abstrahując od możliwych scenariuszy, można z całą pewnością stwierdzić, że rozwiązanie zaproponowane w Projekcie będzie miało negatywne skutki dla przedsiębiorców telekomunikacyjnych i tej części społeczeństwa, która korzysta z ich usług.

Z powyższych względów, KIKE postuluje o ograniczenie skutków decyzji wyłącznie do zakazu wprowadzania nowego sprzętu/oprogramowania do użytkowania i to sprzętu o określonych („zakazanych") parametrach, a nie sprzętu takiego czy innego dostawcy. Sprzęt, który został raz legalnie nabyty, powinien być móc być nadal użytkowany, chyba że przedsiębiorca dobrowolnie zdecyduje się na jego wymianę (np. na podstawie zalecenia, a nie władczego rozstrzygnięcia).

2.6. Pozorność skierowania zakazów jedynie do części przedsiębiorców telekomunikacyjnych

Aktualne rozwiązanie:	część obowiązków związanych z zakazem wprowadzania sprzętu lub oprogramowania do użytkowania i jego wycofaniem została ograniczona do przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń
Proponowane rozwiązanie:	przedsiębiorcy telekomunikacyjni w ogóle nie powinni zostać objęci obowiązkami związanymi z wycofaniem sprzętu lub oprogramowania objętych decyzją

Zgodnie z art. 66a ust. 1 pkt 2, Postępowanie może zostać wszczęte w sprawie uznania za dostawcę wysokiego ryzyka dostawcy sprzętu lub oprogramowania, które wykorzystują *przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.* W uzasadnieniu do Projektu podaje się, że wyżej określone obowiązki nie będą uciążliwe, albowiem jest ok. 100 przedsiębiorców telekomunikacyjnych, którzy spełniają opisane powyżej kryteria, czyli są zobowiązani

[2] https://kike.pl/wp-content/uploads/2020/10/BADANIE-dotyczace-skali-wykorzystania-w-sektorze-telekomunikacyjnym-sprzetu-dostawcow-pochodzacych-spoza-Unii-Europejskiej-lub-Organizacji-Traktatu-Polnocnoatlantyckiego.pdf [dostęp w dniu 03.02.2021 r.]

posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Twórcy Projektu przyjmują zatem, że skutki wyżej opisanej regulacji dotkną jedynie 100 największych przedsiębiorców telekomunikacyjnych. KIKE zwraca uwagę na błąd logiczny w takim rozumowaniu, przekładający się na błędne wnioski, a przede wszystkim na zupełnie niewłaściwą oceną skutków proponowanej regulacji.

Twierdzenie twórców Projektu zostało bowiem oparte na założeniu, że z sieci telekomunikacyjnych, a w szczególności z produktów ICT, usług ICT i konkretnych procesów ICT, należących do dużych operatorów telekomunikacyjnych czy też odbywających się w ich przedsiębiorstwach, korzystają wyłącznie opisywani duzi przedsiębiorcy telekomunikacyjni. Tymczasem, wielu przedsiębiorców telekomunikacyjnych prowadzi działalność telekomunikacyjną, bazując wyłącznie bądź w przeważającej części na dostępie do usług hurtowych świadczonych przez innych przedsiębiorców telekomunikacyjnych. W szczególności, dużą popularnością w zakresie dostępu hurtowego do sieci telekomunikacyjnych cieszą się usługi takie jak usługa BSA, usługa LLU, usługa VULA, usługa transmisji danych, które pozwalają operatorom na świadczenie usług telekomunikacyjnych bez posiadania własnej infrastruktury w danej lokalizacji, a także bez dysponowania personelem na danym terenie. Zdarza się, że operator w zasadzie odsprzedaje swoim abonentom usługę zakupioną w wersji gotowej od operatora sieci dostępowej. Twórcy Projektu w ogóle nie wzięli pod uwagę, iż wyróżnia się warstwę logiczną i warstwę fizyczną sieci.

Korzystanie i świadczenie usług hurtowych jest aktualnie mocno promowane w środowisku telekomunikacyjnym, w szczególności na gruncie realizacji projektów POPC. Przykładowo, w ostatnim czasie CPPC rozpoczęło cykl warsztatów dotyczących *Współpracy z potencjalnymi operatorami korzystającymi w zakresie dostępu do infrastruktury telekomunikacyjnej w sieci POPC*[3] - co ma wpłynąć na rozwój i upowszechnienie usług dostępu hurtowego.

Przytoczone powyżej okoliczności związane z dostępem hurtowym mogą mieć szeroki wpływ na rzeczywiste skutki proponowanej regulacji, albowiem możliwe jest wystąpienie co najmniej czterech opisanych poniżej scenariuszy.

Scenariusz pierwszy – jeśli regulacja zostanie utrzymana w aktualnym kształcie, może dojść do sytuacji, w której duzi operatorzy, objęci nakazem uregulowanym w Projekcie, będą zmuszeni wycofać z użytkowania określone typy produktów. Jeśli produktem tym będą urządzenia udostępnione mniejszym operatorom w celu korzystania przez nich z usług hurtowych (zdarza się bowiem, że przedsiębiorcy telekomunikacyjni korzystający z usług hurtowych, wybierają tą opcję usługi, w której wszelkie urządzenia dostarcza operator sieci dostępowej), to nie sposób wykluczyć sytuacji, w której to właśnie operatorzy korzystający zostaną obciążeni rzeczywistymi kosztami zastosowania się do ustawowych nakazów (tj. kosztami wymiany urządzeń na nowe).

Scenariusz drugi - jeśli regulacja zostanie utrzymana w aktualnym kształcie, może dojść do sytuacji, w której duzi operatorzy, objęci nakazem uregulowanym w Projekcie, będą zmuszeni wycofać z użytkowania określone typy produktów. Możliwe jest, że zmiana używanych w ramach danej sieci telekomunikacyjnej urządzeń może wymagać zmian konfiguracji tej sieci, czy to w warstwie aktywnej czy to w warstwie infrastruktury. Efektem koniecznych modyfikacji w ramach przedsiębiorstwa operatora sieci dostępowej może być *de facto* przymuszenie operatorów korzystających do wymiany urządzeń stosowanych a w ramach ich przedsiębiorstwa.

Chodzi o to, że zdarza się, iż operatorzy korzystający z usług hurtowych świadczonych przez innych przedsiębiorców telekomunikacyjnych, decydują się na tą opcję usługi, która nie obejmuje zapewnienia

[3] https://cppc.gov.pl/dane-dla-operatorow [dostęp w dniu 02.02.2021 r.]

urządzeń wymaganych do świadczenia usług telekomunikacyjnych na rzecz użytkownika końcowego (np. usługa BSA w opcji, w której urządzenie CPE nie jest dostarczane przez operatora sieci dostępowej). W takim przypadku operatorzy korzystający we własnym zakresie zapewniają odpowiednie urządzenia, zaś urządzenia te muszą być kompatybilne z siecią telekomunikacyjną/usługami operatora sieci dostępowej. W praktyce często wygląda to tak, że operatorzy sieci dostępowych udostępniają operatorom korzystającym listę urządzeń, które spełniają wymagane kryteria i których może używać operator korzystający w celu korzystania z usług hurtowych i świadczenia usług telekomunikacyjnych na rzecz swoich abonentów. W opisywanym scenariuszu, pomimo tego, że mali i średni operatorzy nie zostali objęci wprost normą uregulowaną w art. 66b ust. 1-3, to pośrednio dyspozycja tej normy prawnej obejmie także właśnie małych i średnich przedsiębiorców telekomunikacyjnych. Aby dalej korzystać z usług hurtowych dużego przedsiębiorcy, operator korzystający będzie musiał wymienić swoje urządzenia, aby były one kompatybilne z siecią dużego operatora.

Scenariusz trzeci - jeśli regulacja zostanie utrzymana w aktualnym kształcie, może dojść do sytuacji, w której duzi operatorzy, objęci nakazem uregulowanym w Projekcie, będą zmuszeni wycofać z użytkowania określone typy produktów. Możliwe jest, że zmiana używanych w ramach danej sieci telekomunikacyjnej urządzeń nie będzie wymagać żadnych zmian konfiguracji tej sieci, w tym nie będzie wymagać zmiany urządzeń używanych przez operatorów korzystających. Dojdzie zatem do sytuacji, w której usługa na rzecz użytkownika końcowego będzie świadczona np. przez małego ISP (nieobjętego nakazem wycofania urządzeń), bazującego na usłudze BSA świadczonej na jego rzecz przez operatora sieci dostępowej (objętego nakazem wycofania urządzeń), z użyciem własnego CPE dostarczonego przez małego ISP, które to CPE może być urządzeniem, które operator sieci dostępowej miał w ramach swojego przedsiębiorstwa wycofać z użytkowania. Najprościej rzecz ujmując będzie to wyglądać tak, że do sieci dostępowej (objętej nakazem wycofania urządzeń) będzie podłączone urządzenie, którego dostawca został uznany za dostawcę wysokiego ryzyka. Brak będzie bowiem w takiej sytuacji podstawy prawnej do tego, aby wymóc na małym ISP wycofanie tych urządzeń, w szczególności nie sposób przyjąć, aby operator sieci dostępowej miał umownie przewidzieć taki obowiązek po stronie operatora korzystającego. Innymi słowy, w świetle aktualnej treści Projektu, użytkowanie tych urządzeń przez małego ISP będzie dalej legalne. Jak widać, w opisywanym scenariuszu jedynie pozornie zostanie osiągnięty cel, jakiemu przyświeca uregulowanie zawarte w Projekcie, a za jaki należy uznać zapewnienie bezpieczeństwa narodowego.

Scenariusz czwarty - jeśli regulacja zostanie utrzymana w aktualnym kształcie, może dojść do sytuacji, w której duzi operatorzy, objęci nakazem uregulowanym w Projekcie, będą zmuszeni wycofać z użytkowania określone typy produktów. W przypadku, gdy podmioty te będą korzystać z usług hurtowych świadczonych przez przedsiębiorców telekomunikacyjnych nieobjętych wprost tym nakazem, w opcji z urządzeniem dostarczanym przez tych przedsiębiorców telekomunikacyjnych, pośrednim skutkiem nakazu wynikającego z Projektu, będzie obowiązek wycofania z użytku określonych urządzeń także przez przedsiębiorców telekomunikacyjnych pełniących funkcje operatorów sieci dostępowych dla operatorów korzystających objętych wprost analizowanym nakazem.

Kolejno, KIKE zwraca uwagę na art. 66c, zgodnie z którym wszyscy przedsiębiorcy telekomunikacyjni (a nie jedynie ich grupa określona w art. 66a ust. 1 pkt 2 Projektu) *są zobowiązani przekazać informacje na wniosek uprawnionych organów o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ISCT w zakresie objętym decyzją*. Biorąc pod uwagę, że aktualna wersja Projektu organiczna zakres podmiotowy nakazu wycofania wyżej określonych elementów jedynie do określonej kategorii przedsiębiorców telekomunikacyjnych (tj. obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń), objęcie obowiązkiem przekazywania informacji (a zatem *de facto* przekazywania danych o wykonaniu nakazu uregulowanego w Projekcie) wszystkich przedsiębiorców telekomunikacyjnych, jest całkowicie błędne i nieuzasadnione. Nie sposób bowiem określić, z jakich

przyczyn mali i średni przedsiębiorcy mieliby przekazywać informacje np. o wycofaniu określonych urządzeń w zakresie objętym decyzją, o której mowa w art. 66a ust. 8, skoro nie mają obowiązku zastosowania się do decyzji, w szczególności wycofania urządzeń dostawcy objętego tą decyzją. Zdaniem KIKE, art. 66c jest sprzeczny z art. 66b.

2.7. Brak uzasadnienia decyzji oraz wyroku WSA

Aktualne rozwiązanie: możliwość odstąpienia od uzasadnienia decyzji lub wyroku

Proponowane rozwiązanie: brak wprowadzania szczególnych regulacji

W pierwszej kolejności, KIKE podnosi, że wyjaśnienia wymaga, czy w sytuacji, w której minister stwierdzi, że brak jest podstaw do uznania danego dostawcy za dostawcę wysokiego ryzyka jest wydawana decyzja administracyjna, a jeśli nie, to jaką ma formą zakończenie postępowania. W projektowanym art. 66a ust. 8 jest bowiem zapisane, że wydawana jest decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka – a zatem z przepisu tego wynika jedynie, że decyzję wydaje się wówczas, gdy zachodzą przesłanki do uznania dostawcy za dostawcę wysokiego ryzyka.

Projekt przewiduje:

- możliwość odstąpienia od sporządzenia uzasadnienia decyzji w części dotyczącej uzasadnienia faktycznego przez ministra wydającego decyzję uznającą dostawcę za dostawcę wysokiego ryzyka (jak się wydaje, jeśli decyzja będzie odmawiała uznania dostawcy za dostawcę wysokiego ryzyka art. 66a ust. 10 nie będzie miał zastosowania), *jeżeli wymagają tego względy obronności lub bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego*;
- że skarżącemu decyzję ministra doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia *ze względu na ochronę informacji niejawnych*, z czego skarga jest rozpatrywana na posiedzeniu niejawnym, przez co skarżący zostanie pozbawiony możliwości zapoznania się z motywami rozstrzygnięcia przedstawionymi w formie ustnej przez skład orzekający;
- możliwość odstąpienia od sporządzenia uzasadnienia polecenia zabezpieczającego w części dotyczącej uzasadnienia faktycznego przez ministra wydającego polecenia zabezpieczającego, *jeżeli wymagają tego względy obronności lub bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego.*

Odnosząc się wyłącznie do literalnej treści tych regulacji, KIKE podnosi, że gdyby w ogóle rozważać możliwość wyłączenia z jawności pewnej części postępowania czy treści rozstrzygnięć (czemu KIKE kategorycznie się sprzeciwia) należałoby we wszystkich przedstawionych powyżej przypadkach zastosować tożsame przesłanki wyłączenia. Przesłanki te powinny mieć zaś charakter konkretny. Z uwagi na wagę tych przesłanek oraz w celu zapobiegania ewentualnym nadużyciom na tym tle, nie jest dopuszczalne posłużenie się w tym zakresie klauzulami generalnymi czy pojęciami niedookreślonymi.

Zgodnie z zasadą przekonywania wyrażoną w art. 11 KPA:

> *Organy administracji publicznej powinny wyjaśniać stronom zasadność przesłanek, którymi kierują się przy załatwieniu sprawy, aby w ten sposób w miarę możności doprowadzić do wykonania przez strony decyzji bez potrzeby stosowania środków przymusu*.

KIKE zwraca również uwagę na naczelne zasady zapisane w Konstytucji Rzeczypospolitej Polskiej:

> Art. 2:

Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej.

Art. 37 ust. 1:

Kto znajduje się pod władzą Rzeczypospolitej Polskiej, korzysta z wolności i praw zapewnionych w Konstytucji.

Art. 45:

1. Każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy bez nieuzasadnionej zwłoki przez właściwy, niezależny, bezstronny i niezawisły sąd.

2. Wyłączenie jawności rozprawy może nastąpić ze względu na moralność, bezpieczeństwo państwa i porządek publiczny oraz ze względu na ochronę życia prywatnego stron lub inny ważny interes prywatny. Wyrok ogłaszany jest publicznie.

Art. 78:

Każda ze stron ma prawo do zaskarżenia orzeczeń i decyzji wydanych w pierwszej instancji. Wyjątki od tej zasady oraz tryb zaskarżania określa ustawa.

Wyjaśnienie przesłanek, którymi kierował się organ przy rozstrzygnięciu sprawy, następuje poprzez uzasadnienie decyzji. Ważnym elementem tej decyzji jest uzasadnienie faktyczne, bowiem to właśnie stan faktyczny w procesie subsumpcji decyduje o tym, czy możliwe jest w danej sprawie zastosowanie konkretnej normy prawnej. Nie z byle powodu dużą cześć środków odwoławczych stanowią często zarzuty dotyczące błędów w ustaleniach faktycznych. Jeśli skarżący nie będzie mógł się zapoznać z tą częścią uzasadnienia, to w zasadzie zostanie pozbawiony możliwości obrony swoich praw – nie będzie bowiem w stanie ocenić, czy organ prawidłowo ustalił stan faktyczny, a tym samym, czy istniały podstawy do sięgnięcia przez organ do danego przepisu prawa.

Jak zostało podniesione powyżej, w przypadku wyroku wydawanego w rozpatrzeniu skargi, możliwe jest pozbawienie skarżącego możliwości zapoznania się nie tylko z tą częścią uzasadnienia, która obejmuje uzasadnienie faktyczne, ale i z niedookreśloną częścią uzasadnienia, która zdaniem sądu będzie wymagała utajenia. Nie można zatem wykluczyć sytuacji, w której skarżącemu zostanie jedynie udostępniona sentencja wyroku z ewentualnym uzasadnieniem rozstrzygnięcia dotyczącego kosztów postępowania, zaś cała warstwa merytoryczna uzasadnienia, która mogłaby pozwalać skarżącemu na wystąpienie ze skargą kasacyjną, zostanie utajniona.

Co istotne, w żadnym z przytoczonych powyżej przypadków nie zostały przewidziane środki odwoławcze od wyłączenia jawności części postępowania bądź uzasadnień wydawanych rozstrzygnięć. Oznacza to, że *de facto* realność konstytucyjnego prawa skarżącego do sądu będzie uzależniona od jednoinstancyjnej, uznaniowej decyzji danego podmiotu, która nie będzie podlegała kontroli żadnego organu bądź innego podmiotu. Innymi słowy, o wyłączeniu jawności będzie arbitralnie decydował sąd/organ, a skarżący nie będzie mógł zakwestionować tej decyzji.

Uzyskanie uzasadnienia decyzji (i wyroku) jest zaś fundamentalne dla możliwości dochodzenia przez przedsiębiorcę swoich praw. Brak uzasadnienia decyzji/wyroku uniemożliwia przedsiębiorcy uzyskanie informacji o przyczynach podjęcia przez organ/sąd takiego, a nie innego rozstrzygnięcia, a w konsekwencji ogranicza – a wręcz uniemożliwia - przedsiębiorcy, wniesienie odwołania/skargi.

Opisywane uregulowanie będzie miało jeszcze inny skutek. Nie tylko nie będzie możliwe odpowiednie sformułowanie odwołania/skargi, ale i nawet w przypadku wniesienia odwołania/skargi, kontrola rozstrzygnięcia będzie z natury rzeczy ograniczona. Z Projektu nie wynika bowiem, aby jedynie się nie

udostępniało dostawcy uzasadnienia faktycznego decyzji, ale w ogóle ma nie dojść do jego sporządzenia (sic!). Skoro zatem sąd nie będzie znał podstaw faktycznych decyzji, to jak ma sprawdzić, czy te ustalenia nie zawierały błędów, a także czy w ich konsekwencji decyzja jest zasadna? W efekcie, kontrola ograniczy się jedynie do badania kwestii proceduralnych, co w przypadku decyzji tak dalece opartych na uznaniu organu administracyjnego, czyni ochronę zainteresowanego podmiotu – a przede wszystkim możliwość skorzystania przez dostawcę z konstytucyjnego prawa do sądu – całkowicie iluzoryczną.

Co więcej, WSA będzie musiał samodzielnie ustalić od nowa stan faktyczny, skoro nie będzie mógł przyjąć za własne ustaleń faktycznych poczynionych przez organ, co może być znacznie ograniczone, zważywszy na to, że sprawa ma być rozpatrywana na posiedzeniu niejawnym. Biorąc jednak pod uwagę to, że wysoce prawdopodobne jest, że skarżącemu i tak uzasadnienie faktyczne wyroku nie zostanie udostępnione, to nie sposób wykluczyć sytuacji, w których WSA pominie ustalenie stanu faktycznego, jedynie formalne popierając decyzję ministra, nie narażając się na jakiekolwiek konsekwencje w tym zakresie, albowiem skarżący i tak nie będzie miał wglądu do tej części uzasadnienia, a w interesie ministra nie będzie podważanie jakiejkolwiek części rozstrzygnięcia, jeśli będzie ono utrzymywać w mocy decyzję tego organu.

Skoro materialnoprawną podstawą dla wydania decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka ma być przepis projektowanego art. 66a ust. 8, który zawiera jedynie ogólną przesłankę wydania takiej decyzji (tj. *z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego*), nie wskazując (chociażby przez egzemplifikację), jakie sytuacje mają przesądzić o negatywnej ocenie dostawcy, to rezygnacja z uzasadnienia decyzji powinna być niedopuszczalna.

W świetle aktualnej treści Projektu, nie jest jednoznaczne, czy w przypadku wniesienia skargi kasacyjnej Naczelny Sąd Administracyjny będzie dysponował wyrokiem Wojewódzkiego Sądu Administracyjnego wraz z uzasadnieniem. Wydaje się, że projektowany art. 66d ust. 2 nie wyłącza udostępnienia wyroku wraz z pełnym uzasadnieniem Naczelnemu Sądowi Administracyjnego w tym celu, ale kwestia ta może rodzić wątpliwości, przez co wymagane jest jej rozstrzygnięcie w treści konkretnego przepisu.

Nie został zatem rozwiązany problem braku dwuinstancyjności postępowania zidentyfikowany przez KIKE w Poprzednim Projekcie, skoro możliwość odwołania się od decyzji jest iluzoryczna.

W ocenie KIKE, możliwe jest stosowanie innych mechanizmów pozwalających na ochronę obronności lub bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, które jednak zapewnią sądom administracyjnym realną kontrolę działań organu administracji publicznej, a stronie prawo do rzetelnego procesu sądowego. Takim rozwiązaniem może być chociażby nadanie klauzuli niejawności określonym elementom uzasadnienia decyzji/wyroku oraz poddanie kontroli decyzji o nadaniu takiej klauzuli innemu organowi bądź sądowi.

2.8. Natychmiastowa wykonalność decyzji

Aktualne rozwiązanie: decyzja o uznaniu za dostawcę wysokiego ryzyka jest natychmiast wykonalna; sąd administracyjny nie może uchylić rygoru po wniesieniu skargi na decyzję

Proponowane rozwiązanie: przepis dotyczący stosowania rygoru natychmiastowej wykonalności powinien zostać usunięty – decyzja nie powinna być wykonalna do czasu uprawomocnienia się wyroku sądu; względnie nie należy wyłączać możliwości uchylenia rygoru przez sąd administracyjny po wniesieniu skargi

Zakładając, że projektodawca rozwiąże problem indywidualnego charakteru decyzji administracyjnej wydawanej przez ministra w Postępowaniu i bezpodstawnego obarczenia jej skutkami podmiotów trzecich, zasygnalizowany we wcześniejszej części niniejszego stanowiska, nadanie decyzji rygoru natychmiastowej wykonalności, w połączeniu z przewidzianym w Projekcie zakazem wstrzymania wykonalności decyzji przez sąd administracyjny po wniesieniu skargi (projektowany art. 66d ust. 3), doprowadzi do automatycznego i natychmiastowego nakazu rozpoczęcia wycofywania sprzętu/oprogramowania dostawcy uznanego za dostawcę wysokiego ryzyka, zaś produkty, usługi lub procesy ICT dostawcy wskazanego w decyzji nie będą też mogły być nabywane.

Pozostawia to m.in. przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, w niepewności. Z jednej strony, zobowiązani będą do rozpoczęcia wymiany sprzętu/oprogramowania oraz nie będą mogli nabywać tego sprzętu. Z drugiej strony, decyzja nie jest ostateczna i podlega zaskarżeniu do WSA co oznacza, że może zostać uchylona i w konsekwencji **(1)** wymóg wymiany sprzętu/oprogramowania nie będzie istnieć oraz **(2)** dany sprzęt/oprogramowanie mogą zostać zakupione i użytkowane. Późniejsze ewentualne korzystne rozstrzygnięcie sądowe dla wnoszącego skargę nie będzie miało znaczenia, skoro z uwagi na rygor natychmiastowej wykonalności decyzji, sprzęt zostanie usunięty lub nie będzie kupowany od tego dostawcy.

Zgodnie z art. 108 § 1 zd. 1 KPA:

> *Decyzji, od której służy odwołanie, może być nadany rygor natychmiastowej wykonalności, gdy jest to niezbędne ze względu na ochronę zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony.*

Jest to instytucja, która powinna być stosowana wyjątkowo – jedynie wówczas, gdy natychmiastowe niewykonanie decyzji zagraża w sposób konkretny i realny zdrowiu lub życiu ludzkiemu, może spowodować ciężkie straty w gospodarstwie narodowym lub zagrozi innym dobrom, które składają się inny interes społeczny, o jakim mowa w art. 108 § 1 KPA (wyrok WSA w Kielcach z dnia 24 stycznia 2019 r. w sprawie o sygnaturze akt II SA/Ke 612/18). Zważywszy, że projektodawca i tak przewiduje rozłożony w czasie proces wymiany sprzętu, nakaz rygoru natychmiastowej wykonalności jest niezrozumiały i niekonsekwentny – sprzęt nie zniknie z dnia na dzień z użytkowania w sieciach telekomunikacyjnych, lecz za to nie będzie mogło nastąpić rozpoczęcie jego użytkowania.

KIKE postuluje zatem, aby usunąć przewidziany rygor natychmiastowej wykonalności, który może zostać nadany wyłącznie wówczas, gdy spełnione zostaną przesłanki określone w art. 108 KPA. Względnie, w razie nieuwzględnienia powyższej uwagi, KIKE postuluje, aby nie wprowadzać w UKSC szczególnych zasad uchylania rygoru natychmiastowej wykonalności decyzji.

Możliwość wstrzymania wykonalności decyzji przez sąd administracyjny jest jednym z fundamentów sądowej kontroli nad organami administracji. W konsekwencji, wszelkie odstępstwa od tej zasady powinny być szeroko uzasadnione określonymi względami, oraz powinny być niezbędne i proporcjonalne. Wstrzymanie wykonalności decyzji ma znaczenie właśnie w sytuacji, w której zachodzi niebezpieczeństwo wyrządzenia znacznej szkody lub spowodowania trudnych do odwrócenia skutków. Dokładnie taka sytuacja może nastąpić w następstwie zastosowania rozwiązań proponowanych w Projekcie, tj. w następstwie wydania decyzji mogą powstać już nieodwracalne konsekwencje dla strony, jak również innych podmiotów, wobec których decyzja – według Projektu – ma wywoływać określone skutki.

2.9. Transparentność postępowania sądowego

Aktualne rozwiązanie: rozpatrzenie skargi następuje na posiedzeniu niejawnym

Proponowane rozwiązanie: brak wprowadzania szczególnych regulacji dotyczących trybu rozpatrywania skargi

Zaproponowany w Projekcie przepis art. 66d ust. 1 stanowi odstępstwo od kardynalnych zasad nie tylko procedury administracyjnej, ale każdego rzetelnego postępowania, w postaci jego jawności, ustności, prawa do skutecznego wniesienia środka zaskarżenia i generalnie prawa do obrony. Przedsiębiorca objęty postępowaniem będzie mieć ograniczone możliwości obronny swoich praw. Można wręcz stwierdzić, iż w ogóle nie będzie miał realnego prawa do obrony swoich interesów, skoro skarga będzie rozpoznawana na posiedzeniu niejawnym i nie będzie on mógł zapoznać się z pełnym uzasadnieniem wyroku. Dostawcy jedynie pozornie nie pozbawia się prawa do sądu i obrony swoich praw, zaś zagwarantowane mu aktualnie w Projekcie środki, z których może skorzystać w tym celu miałyby taki sam skutek, jak gdyby całkowicie wyłączono zaskarżalność decyzji. Zdaniem KIKE, takie rozwiązanie powinno zostać zaopiniowane przez Komisję Europejską.

Projektodawca wskazał w uzasadnieniu do Projektu, że analogiczne rozwiązanie przewidziane jest w art. 38 ustawy *o ochronie informacji niejawnych*. Wskazany przepis odnosi się jednak do konkretnego postępowania, które regulowane jest ustawą o ochronie informacji niejawnych, tj. postępowania sprawdzającego. **Postępowanie sprawdzające jest całkowicie innym postępowaniem, niż postępowanie, którego celem jest zakazanie sprzedaży swoich produktów przez konkretnego przedsiębiorcę z powodu zagrożenia bezpieczeństwa**. Zdaniem KIKE, jest to analogia kompletnie chybiona. Jedynie na marginesie KIKE zwraca uwagę na wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. w sprawie o sygnaturze akt SK 8/14, w którym Trybunał orzekł, że:

> *Art. 38 ust. 3 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r. poz. 412 i 650) w zakresie, w jakim przewiduje doręczenie skarżącemu odpisu wyroku sądu administracyjnego bez tej części uzasadnienia, której utajnienie nie jest konieczne dla ochrony informacji niejawnych, jest niezgodny z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej oraz z art. 78 w związku z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.*

2.10. Określenie funkcji krytycznych dla bezpieczeństwa sieci (załącznik nr 3 do UKSC)

Aktualne rozwiązanie: ustawowe określenie funkcji krytycznych (załącznik nr 3 do UKSC)

Proponowane rozwiązanie: rezygnacja z określenia funkcji krytycznych (rezygnacja z załącznika nr 3)

Załącznik nr 3, określający funkcje krytyczne dla bezpieczeństwa sieci, jest fundamentalny z punktu widzenia określenia terminu na wycofanie sprzętu (oprogramowania) z użytkowania – 5 czy 7 lat. Szczegółowe uwagi dot. iluzoryczności 7-letniego terminu na wycofanie sprzętu z użytkowania zostały już przedstawione we wcześniejszej części niniejszego pisma, wobec czego nie ma potrzeb ich powielenia. W tym miejscu należy jedynie przypomnieć, że **dobór kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług powoduje, że ISP zawsze będą objęci krótszym, 5-letnim terminem na wycofanie sprzętu z użytkowania.**

Przykładowo:

- uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu będzie obejmować np. konfigurację protokołu PPPoE;
- przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi następuje np. na urządzeniach OLT z Wi-Fi;

- ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm – odbywa się m.in. przy użyciu ONT.

Wszystkie wymienione w załączniku kategorie *funkcji krytycznych* są niezbędnymi elementami sieci telekomunikacyjnej, tyle że na różnych warstwach sieci lub na różnych urządzeniach. Innymi słowy, brak którejkolwiek z funkcji wskazanych w załączniku nr 3, powodowałby zakłócenie funkcjonowania sieci i niemożliwość świadczenia usług telekomunikacyjnych, co nie oznacza, że w kontekście zapewnienia bezpieczeństwa wszystkie elementy sieci są elementami krytycznymi.

Z powyższych względów, utworzenie załącznika wymieniającego *funkcje krytyczne*, mija się z celem, skoro jedynym powodem jego utworzenia jest ustalenie terminu (5 czy 7 lat) na wycofanie sprzętu/oprogramowania z użytkowania. KIKE wnosi o usunięcie tego załącznika, który ma stwarzać pozory istnienia dwóch terminów i „wsłuchania się" ustawodawcy w uwagi krytyczne zgłoszone na etapie konsultacji Poprzedniego Projektu. W przypadku bowiem elementów krytycznych infrastruktury, należy zastosować wyższy poziom bezpieczeństwa, niż w przypadku pozostałych elementów. Składniki są krytyczne w szczególności wtedy, gdy techniczne nieprawidłowości prowadzić mogą do istotnych naruszeń bezpieczeństwa lub naruszeń ochrony danych w znacznym stopniu. Krytyczność danego stopnia jest uzasadniona przez te funkcje, które mogą doprowadzić do nieprawidłowości technicznych w przypadku awarii.

Względnie, dobór funkcji krytycznych powinien nastąpić przy udziale regulatora rynku telekomunikacyjnego oraz przedsiębiorców telekomunikacyjnych, którzy najlepiej znają architekturę sieci telekomunikacyjnych i trafnie potrafiliby zidentyfikować krytyczne elementy sieci i usług.

3. Ostrzeżenia i polecenia zabezpieczające

3.1. Uwagi wstępne

Zastosowanie instytucji *ostrzeżeń* i *poleceń zabezpieczających* (projektowane art. 67a i 67b) wobec operatorów telekomunikacyjnych nie było przewidziane w Poprzednim Projekcie. Jest to nowe rozwiązanie, na tyle istotne, że powinno podlegać ponownym konsultacjom publicznym. Kształtuje ono negatywnie sytuację przedsiębiorców telekomunikacyjnych w stopniu daleko bardziej idącym niż czynił to Poprzedni Projekt. Dlatego KIKE stanowczo sprzeciwia się wprowadzeniu takiego rozwiązania w kształcie zaproponowanym w Projekcie.

3.2. Polecenia zabezpieczające

Rozwiązanie przyjęte w Projekcie nie tylko nie pozwoli na spełnienie oczekiwanego od niego zadania (natychmiastowe wyeliminowanie skutków incydentu cyberzagrożeń), ale niesie za sobą ryzyko natychmiastowego i niemal niekontrolowanego wyeliminowania z rynku określonego sprzętu lub dostawcy.

Zgodnie z projektowanym art. 67b, minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może wydać w drodze decyzji administracyjnej polecenie zabezpieczające w stosunku do m.in. przedsiębiorców telekomunikacyjnych – bez wyjątków. Polecenie zabezpieczające ma zawierać wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Przez wskazanie takiego zachowania rozumie się m.in. **(1)** zakaz korzystania z określonego sprzętu lub oprogramowania, **(2)** nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL, **(3)** nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania. Decyzja ma podlegać natychmiastowej wykonalności, zaś wydaje się ją na czas koordynacji obsługi incydentu krytycznego, nie dłużej niż dwa lata.

Rozwiązanie dotyczące nakazu wycofania sprzętu (oprogramowania) z użytkowania było szeroko krytykowane w procesie konsultacji publicznych. Projektodawca nie rozwiązał tego problemu – a co więcej - zmodyfikował uprzednio zaproponowaną regulację na niekorzyść ISP. Zdaniem KIKE, instytucja polecenia zabezpieczającego stanowi „wprowadzenie tylnymi drzwiami" rozwiązania przewidzianego w Poprzednim Projekcie i to w formie znacznie bardziej rygorystycznej niż pierwotnie zakładano.

Przypomnieć należy, że Poprzedni Projekt przewidywał obowiązek przedsiębiorców telekomunikacyjnych do wycofania sprzętu/oprogramowania z użytkowania w ciągu 5 lat, liczonych od dnia publikacji informacji o decyzji Kolegium o uznaniu dostawcy za stwarzającego zagrożenie. Obecnie, Projekt przewiduje możliwość nakazania wycofania z użytkowania określonego sprzętu lub oprogramowania (tj. zakaz korzystania) w zasadzie z dnia na dzień (art. 67b ust. 3)/

Polecenie zabezpieczające podlega natychmiastowej wykonalności.

Oznacza to, że w razie wydania takiego polecenia przedsiębiorca z dnia na dzień będzie zmuszony zaprzestać korzystania z określonego sprzętu/oprogramowania, co może mieć katastrofalne skutki dla ISP.

KIKE postuluje, aby zrezygnować z instytucji polecenia zabezpieczającego na rzecz instytucji ostrzeżeń, zawierającej postulaty określonego zachowania, wskazujących ryzyka. ISP najlepiej wiedzą, jak wygląda architektura i konfiguracja ich sieci. Aby móc w pełni zabezpieczyć ją przez wystąpieniem incydentów, zasadne jest, aby byli ostrzegani o możliwości wystąpienia takich incydentów, jednakże sposób i metody zabezpieczenia sieci powinny pozostać w gestii każdego ISP. Kwestia cyberbezpieczeństwa nie jest tą, którą można skutecznie zarządzać na poziomie centralnym. Zróżnicowanie wykorzystywanego sprzętu, oprogramowania i wykorzystywanych rozwiązań jest tak rozległe, że nie da się skutecznie wydawać poleceń na poziomie centralnym (przez ministra). Niejednokrotnie wystąpienie incydentu wymaga natychmiastowego podjęcia działań przez samego zainteresowanego i dotkniętego atakiem przedsiębiorcę. Rozwiązanie przewidujące wydawanie poleceń przez organ centralny z punktu widzenia cyberbezpieczeństwa jest całkowicie chybione i pozbawione sensu.

4. Zmiany w prawie telekomunikacyjnym

W art. 2 Projektu dodaje się do UstPT nową regulację art. 115^4, zgodnie z którą Prezes UKE może zapewnić odpowiednie częstotliwości w celu oferowania przez przedsiębiorcę telekomunikacyjnego na zasadach niedyskryminacyjnych usług na warunkach hurtowych w celu ich dalszej sprzedaży przez innego przedsiębiorcę telekomunikacyjnego. Aktualnie proponowana regulacja wymaga zmian z uwagi na to, że jest niezrozumiała. Nie sposób bowiem określić:

- czy w art. 115^4 chodzi o dalszą odsprzedaż częstotliwości przez wyznaczonego przedsiębiorcę na warunkach rynkowych na rzecz innych przedsiębiorców telekomunikacyjnych, tj. o doprowadzenie do sytuacji, w której to wyznaczony operator telekomunikacyjny (nie zaś Prezes UKE) będzie dysponował określonym pasem częstotliwości i decydował o jego przyznaniu (odsprzedaniu) konkretnemu przedsiębiorcy, zaś samo przyznanie/odsprzedanie będzie się odbywało na podstawie umowy cywilnoprawnej. Czy też o świadczenie usług hurtowych z wykorzystaniem tych częstotliwości przez wyznaczonego przedsiębiorcę na rzecz innych przedsiębiorców telekomunikacyjnych;
- w jakiej formie Prezes UKE ma zapewnić przedsiębiorcy wyznaczonemu odpowiednie częstotliwości (nie wiadomo, czy ma to być forma decyzji administracyjnej oraz jak ta decyzja miałaby się do umowy odsprzedaży częstotliwości);
- jak rozumieć pojęcie *odpowiednich częstotliwości* użyte w art. 115^4 ust. 4;

- czy przepis wyklucza świadczenie usług hurtowych na rzecz innych przedsiębiorców przez przedsiębiorcę, który nie zostanie wyznaczony w trybie art. 115^4 ust. 4, dysponującego częstotliwościami;
- czy przedsiębiorcą wyznaczonym do świadczenia usług, o których mowa w 115^4 ust. 1, może zostać każdy przedsiębiorca telekomunikacyjny, czy też wyłącznie operator sieci komunikacji strategicznej. Zgodnie z Projektem, art. 59ze ma zastrzegać prawo operatora sieci komunikacji strategicznej do świadczenia usług telekomunikacyjnych w oparciu o zasoby częstotliwości, o których mowa w art. 115^4 UstPT.
- czy z odpowiednich częstotliwości, o których mowa w art. 115^4 ust. 1, może skorzystać każdy przedsiębiorca telekomunikacyjny, czy tylko wyznaczony w sposób określony art. 115^4 ust. 4;
- jakie warunki powinien spełnić przedsiębiorca telekomunikacyjny, aby zostać wyznaczonym w sposób określony art. 115^4 ust. 4;
- dlaczego w omawianej regulacji wprowadzono uznaniowość w zakresie decyzji Prezesa UKE o zapewnieniu częstotliwości (przepis stanowi o tym, że Prezes UKE może zapewnić częstotliwości).

***

Karol Skupień Łukasz Bazański Kamila Mizera Anna Szura