Uchwała nr 92
strony pracowników i strony pracodawców
Rady Dialogu Społecznego
z dnia 17 grudnia 2020 roku
w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych

Na podstawie art. 29 w związku z art. 2 pkt 2 ustawy z dnia 24 lipca 2015 r. o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego (tj. Dz. U. z 2018 r., poz. 2232 z późn. zm), uchwala się, co następuje:

§ 1.

Minister Cyfryzacji opublikował 8 września br. *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (UD68)* („**Projekt**").

W myśl uzasadnienia do Projektu celem zmian legislacyjnych jest rozwój krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawnych dotyczących cyberbezpieczeństwa. Niewątpliwie rozwój systemu i zwiększenie cyberbezpieczeństwa jest istotne z punktu widzenia polskiej gospodarki i jej konkurencyjności w świecie, niemniej jednak niektóre z planowanych środków są nieadekwatne i jako takie pociągną za sobą konsekwencje odmienne od oczekiwanych. Poza zmianami dotyczącymi ściśle kwestii związanych z cyberbezpieczeństwem, pojawiają się nowe uregulowania, dotychczas nie występujące w polskim systemie prawnym, a dotyczące „oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa" przez Kolegium (art. 1 punkt 29 Projektu). Są one bardzo istotne, gdyż tego rodzaju oceny prowadzić będą do wiążącego kształtowania polityki zakupowej w zakresie sprzętu i oprogramowania przedsiębiorców telekomunikacyjnych. Ich konsekwencją będzie istotne ograniczenie konkurencji na rynku, a być może być w skrajnym przypadku wyeliminowanie z rynku konkretnego podmiotu gospodarczego.

Zwracamy uwagę, iż planując nową regulację, w ogóle nie wskazuje się na ich skutki ekonomiczne lub finansowe, podczas gdy Projekt będzie miał istotny wpływ nie tylko na operatorów i dostawców, ale również na inne podmioty gospodarcze oraz całe społeczeństwo, a jego koszty będą one liczone w miliardach złotych.

W zakresie skutków Projektu na budżet Polski i gospodarkę krajową wskazać należy, iż Projekt będzie miał negatywny wpływ na gotowość podmiotów do składania ofert na pasma częstotliwości 5G. Fakt niemożności wybrania dostawcy sprzętu lub usług odroczy uruchomienie sieci 5G oraz rozwój Przemysłu 4.0. Według analizy wymiarów strat (aktywów, dodatkowych kosztów migracji, zwiększonej niestabilności OPEX oraz sieci), bezpośrednie straty operatorów przekroczą 2,5 mld euro. Jednocześnie, Projekt ten przyniesie 8,5 mld euro straty w sektorze ICT (wzrost cen z powodu braku konkurencji) oraz ponad 10 mld euro straty w całej gospodarce (lokalne zatrudnienie, zamówienia publiczne, negatywny wpływ na PKB).

Nie bez znaczenia dla polskiej gospodarki pozostaje również fakt, iż wykluczone podmioty gospodarcze będą uprawnione do dochodzenia odszkodowania od Skarbu Państwa. Roszczenia odszkodowawcze operatorów i dostawców wobec Skarbu Państwa zostaną ostatecznie wypłacone przez podatników i konsumentów. Budżet państwa będzie zasilał operatorów i producentów zamiast ułatwiać życie obywatelom, szczególnie po pandemii.

W zakresie skutków społecznych należy opisać wpływ Projektu na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce.

W świetle powyższych skutków regulacji, nie budzi zdziwienia negatywne przyjęcie Projektu przez przedsiębiorców, a w środowisku związanym z rynkiem telekomunikacyjnym kształtujący się pogląd, że podstawowym celem noweli KSC nie jest zmniejszenie zagrożeń związanych z cyberbezpieczeństwem (cel uboczny), ale wyeliminowanie konkretnego dostawcy sprzętu telekomunikacyjnego i zmniejszenie w ten sposób konkurencji na rynku dostawców.

W kontekście oceny dostawców i wykluczenia ich sprzętu oraz oprogramowania, istotnym jest ocena prawna planowanych przepisów, a przede wszystkim zarzut ich niekonstytucyjności, tworzący również na przyszłość niebezpieczny precedens dla dalszego rozwoju prawa gospodarczego w Polsce. Przepisy dotyczące oceny dostawców naruszają zasady przyzwoitej legislacji, zasadę zaufania obywateli do państwa i wynikające z niej zasadę ochrony praw nabytych oraz zasadę niedziałania prawa wstecz (art. 2 Konstytucji), ponadto zasadę wolności działalności gospodarczej (art. 20 i art. 22 Konstytucji) oraz zasadę równości i zakaz dyskryminacji (32 Konstytucji).

Jednym z kryteriów postępowania w sprawie oceny dostawcy prowadzonego przez Kolegium jest prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego (art. 66a ust. 3 pkt 2 Projektu). Tym samym postępowanie opiera się na hipotezach (możliwości i prawdopodobieństwie), nie na faktycznym zagrożeniu. Projektowane kryteria procedury ocennej, której efektem są ogromne konsekwencje dla dostawcy, zostały określone w sposób nieprecyzyjny. Nie odpowiada to zasadzie prawidłowej legislacji wywodzonej z art. 2 Konstytucji.

Postępowanie w sprawie oceny odbywa się w całości bez udziału dostawcy, który dopiero z komunikatu w Monitorze Polskim dowiaduje się, o przeprowadzonej ocenie. Projektowane rozwiązania legislacyjne są nieproporcjonalne do celów zmiany, co przeczy zasadzie demokratycznego państwa prawnego (art. 2 Konstytucji). Należy zauważyć, iż w prawie polskim obowiązuje szereg procedur weryfikujących działalność przedsiębiorców, które w sposób obiektywny, a jednocześnie skuteczny realizują swoje cele. Do tego typu postępowań zaliczyć można np. ogólną kontrolę działalności przedsiębiorcy oraz kontrolę podatkową – postępowanie sprawdzające prawidłowość uiszczania przez przedsiębiorcę danin publicznoprawnych. I tak zgodnie z brzmieniem art. 50 ust. 1 ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców czynności kontrolne wykonuje się w obecności przedsiębiorcy lub osoby przez niego upoważnionej. Przedsiębiorca może wnieść sprzeciw wobec podjęcia i wykonywania przez organ kontroli czynności z naruszeniem przepisów (art. 59 ust. 1 ustawy – Prawo przedsiębiorców). Również kontrola podatkowa zazwyczaj jest czynnością zapowiedzianą. Podatnik powinien otrzymać zawiadomienie o wszczęciu kontroli nie później niż 7 dni przed jej rozpoczęciem. Nie bez znaczenia jest również fakt, iż cała procedura kontrolna została uregulowana w 29 artykułach ustawy z dnia 29 sierpnia 1997 r. Ordynacja podatkowa. Natomiast procedura oceny dostawcy zawarta w Projekcie zajmuje 3 artykuły, a Kolegium ma inwazyjną, niczym nie ograniczoną, opartą na niejasnych kryteriach kompetencję do prowadzenia jednostronnego postępowania ocennego. W krajowym porządku prawnym jedynie organy ścigania posiadają kompetencję do prowadzenia postępowania przygotowawczego, w tym podejmowania czynności operacyjnych bez udziału podejrzanego, pod warunkiem, że w stosunku do takiej osoby zachodzi uzasadnione podejrzenie popełnienia przestępstwa. Dlatego też przyjęte rozwiązania legislacyjne są sprzeczne z zasadą proporcjonalności wyprowadzoną z zasady demokratycznego państwa prawnego.

Projektowana regulacja nie określa żadnych konsekwencji dla organu opiniodawczego za naruszenia przepisów prawa w toku postępowania ocennego lub błędną ocenę. Dla porównania warto ponownie odnieść się do ustawy – Prawo przedsiębiorców, zgodnie z którą przedsiębiorcy, który poniósł szkodę na skutek wykonania czynności kontrolnych z naruszeniem przepisów prawa, przysługuje odszkodowanie (art. 46 ust. 1 ustawy – Prawo przedsiębiorców). Z tego względu projektowany przepis art. 66a ust. 6 Projektu narusza wolność działalności gospodarczej zagwarantowaną w art. 20 i 22 Konstytucji.

Zgodnie z treścią art. 22 Konstytucji, podejmowanie, wykonywanie i zakończenie działalności gospodarczej jest wolne dla każdego na równych prawach, z zachowaniem warunków określonych przepisami prawa. Jakiekolwiek ograniczenie działalności gospodarczej może zostać usankcjonowanie wyłącznie w ustawie, przy czym dla swej prawidłowości musi ona wyraźnie wskazywać na przewidziane prawem warunki prowadzenia działalności gospodarczej.

Projekt przewiduje, iż wyłącznie dostawcy, którego działalność określono na wysoce ryzykowną, przysługuje prawo do złożenia odwołania. Legitymowanym do rozpoznania odwołania jest Kolegium, czyli organ, który wydał ocenę. Projektowane rozwiązanie nie gwarantuje obiektywnej i rzetelnej kontroli oceny, z tego względu naruszona zostaje zasada zaufania obywateli do państwa wynikające z art. 2 Konstytucji oraz art. 32 Konstytucji, z którego wywodzi się zasadę równości wobec prawa, prawo do równego traktowania przez władze publiczne oraz zakaz dyskryminacji.

Niewątpliwie, każda ocena w projektowanej gradacji działalności ryzykownych, wydana po przeprowadzeniu subiektywnego postępowania ocennego będzie dla dostawców szkodliwa. Z tego względu zarówno działalność dostawcy określona jako wysoce ryzykowna, umiarkowanie ryzykowna jak i niskiego ryzyka powinna zostać poddana kontroli. Wszystkich dostawców, w stosunku do których wszczęto postępowanie ocenne działają w tej samej branży. Dostawcy ci są dla siebie konkurencyjni, z tego względu każdy z tych dostawców powinien mieć zagwarantowana w ustawie szansę zweryfikowania przeprowadzonej oceny i w razie jej zmiany lub uchylenia odzyskania zaufania kontrahentów i klientów. Nieuzasadnione pozbawienie części ocenianych dostawców prawa do kontroli instancyjnej oceny stanowi o nierównym traktowaniu dostawców. Ty bardziej, że dostawcy, którzy otrzymali ocenę „umiarkowane ryzyko" mają zakaz wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie. Brak prawa do kontroli oceny czyni ww. zakaz ostatecznym.

Ponadto, projektowana regulacja polegająca na obowiązku wycofania wszystkich produktów, oprogramowania i usług określonych w ocenie narusza zasadę zaufania obywateli do państwa oraz zasadę ochrony praw nabytych wyinterpretowanych z art. 2 Konstytucji. Dotychczas przedsiębiorcy telekomunikacyjni sami decydowali, jakie rodzaje środków technicznych i organizacyjnych chcą zastosować, aby zapewnić bezpieczeństwo sieci i usług telekomunikacyjnych. W związku z powyższym, w myśl ww. zasad ustawodawca nie ma legitymacji do ingerowania w dotychczas prowadzoną działalność podmiotów. Projekt zakłada rażąco niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy, co stanowi naruszenie zakazu działania prawa wstecz.

Projektowane przepisy, w tym zamiar powołania CSIRT Telco, stanowią propozycję pilnego wprowadzenia zupełnie nowego reżimu prawnego i organizacyjnego funkcjonowania przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa. Koncepcja ta zdaje się przy tym pomijać obiektywny fakt, że sektor ten jest i tak znacząco obciążony z uwagi na najpierw opóźnione, a ostatnio prowadzone w dużym tempie zmiany całego systemu prawnego w ramach przyjęcia nowego Prawa Komunikacji Elektronicznej, które, mimo, że wciąż jest na etapie prac rządowych, ma obowiązywać już od 21 grudnia br. Analiza przedłożonego projektu oraz uzasadnienia w tym zakresie wskazuje, że głównym celem i identyfikowanym brakiem jest deficyt odpowiedniej informacji o incydentach dotyczących komunikacji elektronicznej po stronie CSIRT krajowych oraz operatorów usług kluczowych. Takie wnioski są o tyle zastanawiające, że już dzisiaj w reżimie prawnym Prawa telekomunikacyjnego, przedsiębiorca telekomunikacyjny jest zgodnie z art. 175a ust. 1 obowiązany niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych. Jednocześnie, w celu zapewnienia odpowiednich informacji dla podmiotów krajowego systemu cyberbezpieczeństwa, zgodnie z art. 175a ust. 1a dodanym właśnie ustawą o krajowym systemie cyberbezpieczeństwa z 2018 r., obowiązkiem Prezesa UKE, jest przekazywanie informacji o naruszeniach, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego. Co więcej, Prezes UKE ma możliwość korzystania z systemu informatycznego tworzonego na potrzeby krajowego systemu cyberbezpieczeństwa (art. 46 KSC). Konsultowany już projekt PKE utrzymuje te kluczowe rozwiązania i to one powinny być w pierwszej kolejności rozważane. Oznacza to, że już istnieje mechanizm raportowania i przekazywania informacji o incydentach w obszarze

telekomunikacji, które mają wpływ na cyberbezpieczeństwo. Jeśli ten mechanizm nie funkcjonuje zgodnie z oczekiwaniami, należy rozważyć jego dostosowanie, a nie **wprowadzanie drugiego,** na poziomie przepisów potencjalnie zbliżonego mechanizmu raportowania przedsiębiorców do CSIRT.

W związku z powyższym występujemy z następującymi postulatami:

- należy zaniechać szkodliwego dla polskiej gospodarki wykluczania dostawców na podstawie przepisów zawierających nieprecyzyjne kryteria i naruszających przepisy Konstytucji;
- należy wprowadzić oceny urządzeń i oprogramowania o statusie krytycznych tj. mających bezpośredni wpływ na cyberberbezpieczeństwo, w oparciu o precyzyjnie określone, jasne, niebudzące wątpliwości i weryfikowalne kryteria;
- określając zasady bezpieczeństwa dla sprzętu i oprogramowania, należy koncentrować się na normach technicznych i normach certyfikacji, które powinny zostać wprowadzone – takich jak NESAS czy system certyfikacji ENISA, lub inne międzynarodowe lub uznane przez UE norm bezpieczeństwa cybernetycznego, takie jak ISO27001, Common Criteria, Network Equipment Security Scheme, unijny program certyfikacji cyberbezpieczeństwa;
- należy wprowadzić mechanizmy zapewnienia integralności dostarczanych urządzeń i oprogramowania m.in. przez możliwość sprawdzenie w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione, prowadzenie monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych, zatrudnianie tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie, zapewnienie w odpowiednim zakresie redundancji, wskazanym w procedurze bezpieczeństwa, krytycznych składników infrastruktury;
- należy zastosować sprawdzone mechanizmy takie jak deklaracje wiarygodności od producentów i dostawców, zawierające:
  (i) zobowiązanie do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;

(ii) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim;

(iii) obowiązek producenta lub dostawcy infrastruktury telekomunikacyjnej polegający na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;

(iv) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej;

(v) deklarację gotowości do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;

(vi) zapewnienie, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;

(vii) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa;

- wszelkie mechanizmy ocenne należy oprzeć na istniejących przepisach, takich jak te zawarte w ustawie Prawo przedsiębiorców oraz ustawie Kodeks postępowania administracyjnego, opartych na przejrzystych zasadach, umożliwiających udział dostawcy w postępowaniu oraz zapewniających niedyskryminującą procedurę odwoławczą;
- należałoby zrezygnować w projekcie z przepisów dotyczących objęcia przedsiębiorców komunikacji elektronicznej nowymi obowiązkami w ramach ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie włączenia ich do krajowego systemu cyberbezpieczeństwa oraz wprowadzenia nowego reżimu raportowego w zakresie incydentów. Szczególnie, że istnieje już właściwy dla takich podmiotów kanał raportowania do Prezesa Urzędu Komunikacji Elektronicznej, a następnie do podmiotów krajowego systemu cyberbezpieczeństwa.

§ 2.

Uchwała wchodzi w życie z dniem podjęcia.

Uchwała przyjęta podczas posiedzenia plenarnego Rady Dialogu Społecznego w dniu 17 grudnia 2020 r.