Warszawa, dn. 2 listopada 2021 r.

Stanowisko Związku Przedsiębiorców i Pracodawców ws. projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dn. 12.10.2021 r.)

Proces legislacyjny dotyczący projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa trwa już od drugiej połowy 2020 roku, a sam tekst ulegał kilkukrotnym zmianom. Związek Przedsiębiorców i Pracodawców uczestniczył już w konsultacjach przedmiotowego projektu, jednak z uwagi na pojawienie się jego najnowszej, zaktualizowanej wersji, uważamy za stosowne ponowne zajęcie stanowiska wobec przedstawionego do konsultacji dokumentu.

W pierwszej kolejności należy zaznaczyć, że postępująca digitalizacja, którą uważamy za konieczność i gigantyczną szansę dla przyspieszenia rozwoju polskiej gospodarki – przy wszystkich jej zaletach – generuje również nowe rodzaje nieznanych wcześniej ryzyk. Coraz powszechniejsze wykorzystywanie narzędzi cyfrowych np. w sektorze bankowym, administracji publicznej, czy systemie opieki zdrowotnej, sprawia że korzystanie z kluczowych dla obywateli usług staje się znacznie wygodniejsze, a rosnąca liczba dostępnych funkcjonalności po prostu ułatwia życie. W okresie głębokiego lockdownu digitalizacja okazała się w zasadzie jedynym możliwym sposobem utrzymania regularnego rytmu życia zawodowego, czy towarzyskiego.

Firmy dostrzegły w cyfryzacji szansę i coraz częściej decydują się na wykorzystywanie narzędzi cyfrowych w celu usprawnienia i optymalizacji procesów. W potoku tych aktywności generowana jest ogromna ilość danych – często bardzo wrażliwych, a utrata kontroli nad narzędziami cyfrowymi wykorzystywanymi np. w energetyce, czy bankowości, mogłaby nieść za sobą katastrofalne skutki. Tym samym, kluczowe staje się już nie tylko zapewnienie fizycznego bezpieczeństwa nośników danych i elementów infrastruktury, lecz również zabezpieczenie sieci i systemów przed atakami o charakterze cybernetycznym. Dlatego też trudno poddawać w wątpliwość zasadniczy cel projektowanej nowelizacji, jakim jest zwiększenie poziomu cyberbezpieczeństwa państwa.

Jest to szczególnie istotne w kontekście wdrażania standardu 5G, który stanowi fantastyczny instrument dalszego rozwoju narzędzi cyfrowych i poprawy jakości życia. Pełne wykorzystanie potencjału innowacji, które mogą powstać dzięki możliwości bezprzewodowej wymiany ogromnych wolumenów danych w czasie rzeczywistym (bez latencji) będzie jednak możliwe jedynie wówczas, gdy zapewnimy absolutną szczelność i bezpieczeństwo infrastruktury. Jest to istotne tym bardziej, że niepożądane ingerencje w ramach cyberprzestrzeni mogą mieć charakter nie tylko bardziej lub mniej groźnych ataków zorganizowanych, prywatnych grup, lecz mogą stanowić również w praktyce element działań wojennych.

Mając na uwadze powyższe, konieczność wprowadzenia regulacji, które minimalizowałyby ryzyko występowania incydentów zagrażających cyberbezpieczeństwu Polski, jest absolutnie oczywista.

Istotna część proponowanych przepisów jest tym samym niewątpliwie słuszną odpowiedzią na zarysowane wyżej wyzwania – zrozumiałe jest zarówno zaproponowanie przepisów wprowadzających centra wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa, jak i choćby wzmocnienie finansowe i kompetencyjne właściwych organów administracji państwowej.

Niezależnie od powyższego, ważną częścią projektu są naturalnie przepisy dotyczące możliwości uznania konkretnego dostawcy sprzętu za dostawcę wysokiego ryzyka i w konsekwencji konieczności wycofania z użytku sprzętu lub oprogramowania pochodzącego od tegoż dostawcy. Jak niejednokrotnie już zaznaczaliśmy w poprzednich opiniach do omawianego projektu, generalne podejście polskiego regulatora jest dla nas zrozumiałe. W kontekście dynamicznie zmieniającej się sytuacji geopolitycznej i szerokiej debaty toczącej się w wielu państwach członkowskich UE, dotyczącej konieczności zapewnienia bezpieczeństwa infrastruktury wykorzystywanej na potrzeby sieci 5G (której przejawem był również „5G Toolbox"), polski rząd wydaje się dążyć do zapewnienia sobie pola manewru i możliwości podjęcia różnych decyzji, w zależności od kierunku biegu wydarzeń na arenie międzynarodowej. Podtrzymujemy zrozumienie tych założeń, ponownie zwracamy jednak uwagę na konieczność zapewnienia, że przewidziane w ustawie procedury nie będą jednak abstrahowały od gwarancji i reguł obowiązujących na podstawie ustaw takich jak Prawo przedsiębiorców, czy kodeks postępowania administracyjnego. Jest to istotne tym bardziej, że przewidziane kryteria decydujące o uznaniu danego dostawcy za dostawcę wysokiego ryzyka, mają charakter oczywiście oceny i nieprecyzyjny. Niestety, przedstawiony projekt ustawy w dalszym ciągu nie realizuje w pełni wskazanego wyżej założenia.

Projekt przewiduje bowiem, że w toku postępowania w sprawie uznania danego dostawcy za dostawcę wysokiego ryzyka, zastosowania nie znajdzie szereg przepisów kodeksu postępowania administracyjnego. Przede wszystkim, projekt zakłada, że stroną postępowania będzie wyłącznie dany dostawca, którego postępowanie dotyczy – wyłącza się zatem zastosowanie zawartej w art. 28 kpa zasady, zgodnie z którą stroną jest każdy, czyjego interesu prawnego lub obowiązku dotyczy postępowanie. W przypadku tego konkretnego postępowania, taką stroną mógłby być np. przedsiębiorca telekomunikacyjny. Projekt wyklucza również możliwość dopuszczenia do udziału w postępowaniu zainteresowanych organizacji społecznych. Samo wydanie opinii przez Kolegium, na podstawie której minister właściwy ds. cyfryzacji może zadecydować o uznaniu dostawcy za dostawcę wysokiego ryzyka, wyłączone jest z rygoru art. 106 §5 kpa, co powoduje że stanowisko Kolegium nie jest zajmowane w drodze postanowienia, a zatem nie przysługuje na nie również zażalenie. Co więcej, od decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, w myśl projektu nie będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy. Sama decyzja ma mieć zatem – z mocy ustawy – rygor natychmiastowej wykonalności, od którego minister właściwy ds. cyfryzacji nie będzie mógł odstąpić, oraz którego sąd administracyjny nie będzie mógł uchylić.

Wszystko to składa się na sytuację, w której regulator dążąc do osiągnięcia słusznych celów i chcąc zabezpieczyć sobie odpowiednio szerokie pole manewru, nie zapewnił niezbędnych gwarancji proceduralnych podmiotom gospodarczym będącym potencjalnymi podmiotami regulowanych postępowań. Z uwagi na doniosłe skutki decyzji podejmowanych w ramach tych postępowań,

konieczna wydaje się rewizja proponowanych przepisów, wskutek której podmioty posiadające interes prawny miałyby zagwarantowane podstawowe prawa, takie jak np. prawo do bycia wysłuchanym, czy prawo do uzyskania uzasadnienia podjętej decyzji.