OPINIA

KRAJOWEJ RADY SĄDOWNICTWA

z 13 czerwca 2018 r.

w przedmiocie rządowego projektu ustawy o krajowym systemie cyberbezpieczeństwa

Krajowa Rada Sądownictwa, po zapoznaniu się z projektem ustawy o krajowym systemie cyberbezpieczeństwa, przekazanym przy piśmie Zastępcy Szefa Kancelarii Sejmu z 7 maja 2018 r. (GMS-WP-173-140/18) zwraca uwagę na częściowo przecinający się zakres przedmiotowy projektowanej ustawy z obowiązującą ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 ze zm., dalej: ustawa o zarządzaniu kryzysowym). Zauważyć bowiem należy, że uwzględniając projektowane przepisy, usługi kluczowe zależne od systemów teleinformatycznych będą objęte rygorami wynikającymi z uwzględnienia ich w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy sporządzanej na podstawie kryteriów wskazanych w ustawie o zarządzaniu kryzysowym.

Z tych względów projekt powinien przewidywać mechanizmy koordynacji systemu ochrony infrastruktury krytycznej wynikającej z ustawy o zarządzaniu kryzysowym z projektowanym systemem cyberbezpieczeństwa. Odpowiednie mechanizmy powinny zostać przewidziane nie tylko na poziomie właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej i operatorów usług kluczowych, ale również na poziomie organów koordynujących działania podejmowane na podstawie ustawy
o zarządzaniu kryzysowym i organów właściwych do spraw cyberbezpieczeństwa w rozumieniu art. 41 projektowanej ustawy. Wątpliwości Rady budzi przede wszystkim dualizm regulacji w zakresie przyjętej właściwości odnośnie do konkretnych systemów i usług teleinformatycznych. Nieuwzględnienie zasad właściwości organów wynikających z ustawy
o zarządzaniu kryzysowym doprowadzi do sytuacji w której kwalifikacji tych samych usług dokonywać będą różne podmioty. W przypadku uznania, w obu ustawowych reżimach, właściwości przez różne organy, odnośnie do tego samego systemu teleinformatycznego dojdzie do zakłócenia w systemie zapewniania bezpieczeństwa tych systemów.

Zdaniem Rady uwzględnić należy odrębności w zakresie procedury kwalifikowania obiektów, instalacji urządzeń i usług wchodzących w skład infrastruktury krytycznej (niewymagającej wydania decyzji administracyjnej) względem przewidzianej przez projektowany art. 5 decyzji administracyjnej, wydanie której otworzy drogę do kontroli sądowo-administracyjnej, w efekcie której może zaistnieć stan w którym usługa kluczowa zaliczona do infrastruktury krytycznej nie zostanie uznana za usługę kluczową.

Z tego względu projektodawca powinien rozważyć czy zasadnym nie byłoby, w procedurze uznawania podmiotu za operatora usługi kluczowej, wyłączenie postępowania administracyjnego i drogi sądowej poprzez ograniczenie kwalifikacji do złożenia wniosku przez właściwy organ o dokonanie wpisu do wykazu operatorów usług kluczowych, tj. analogicznie do rozwiązania obowiązującego w odniesieniu do infrastruktury krytycznej. Znajduje to uzasadnienie w charakterze usług kluczowych – są to usługi, które ze swojej istoty muszą podlegać ochronie według reguł cyberbezpieczeństwa, zaś ustawa o cyberbezpieczeństwie, porządkując zasady ochrony, nie będzie stanowić ograniczenia praw i wolności operatorów usług kluczowych. Konieczna wydaje się zatem zmiana art. 5 i 7 projektowanej ustawy.

Krajowa Rada Sądownictwa zwraca także uwagę na kwestię wyłączenia jawności jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. Brak analogicznej regulacji, w projektowanej ustawie, odnośnie do usług kluczowych stanowić będzie zagrożenie ujawnienia obiektów infrastruktury krytycznej.

Rada podkreśla także, że stosownej zmiany wymaga projektowany art. 55, albowiem w zakresie w jakim przepis ten miałby znajdować zastosowanie do infrastruktury sądów konieczne jest ograniczenie dostępu, w ramach czynności kontrolnych, wyłącznie do dokumentów z zakresu cyberbezpieczeństwa.