Wstęp

Oddawany do rąk Czytelnika Komentarz do ustawy o krajowym systemie cyberbezpieczeństwa jest wspólnym dziełem ośmiu autorów, pracowników naukowych i praktyków prawa zajmujących się problematyką ochrony cyberprzestrzeni, a w szczególności analizą narzędzi, instytucji i instrumentów prawnych służących zapewnieniu bezpieczeństwa w cyberprzestrzeni rozumianego jako zarówno bezpieczeństwo przesyłu oraz wymiany danych i informacji (treści cyfrowych), jak i bezpieczeństwo świadczenia usług na odległość z wykorzystaniem systemów informatycznych (usługi świadczone drogą elektroniczną), realizowanych przez operatorów usług kluczowych jako posiadających istotne znaczenie dla bezpieczeństwa państwa i jego obywateli oraz usług realizowanych na indywidualne żądanie użytkowników Internetu przez dostawców usług cyfrowych.

Stworzenie spójnego systemu mającego zapewnić cyberbezpieczeństwo Rzeczypospolitej Polskiej było celem uchwalonej przez Sejm RP 5.7.2018 r. ustawy o krajowym systemie cyberbezpieczeństwa, która następnie weszła w życie 28.8.2018 r. Powstał w ten sposób system z jasnym przydziałem zadań i określeniem odpowiedzialności podmiotów wchodzących w jego skład, który miał na celu umożliwienie sprawnego działania na rzecz wykrywania, zapobiegania i minimalizowania skutków incydentów sieciowych (takich jak np. ataki sieciowe lub awarie) naruszających cyberbezpieczeństwo państwa i jego obywateli. Ustawa oraz towarzyszące jej rozporządzenia wykonawcze w pełni wdrożyły do polskiego porządku prawnego postanowienia tzw. dyrektywy NIS [dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii].

Ustawodawca nieprzypadkowo używa w tytule ustawy pojęcia „system cyberbezpieczeństwa". W zamyśle racjonalnie działającego ustawodawcy pozostawało bowiem zbudowanie skoordynowanego mechanizmu wykrywania, powiadamiania i reagowania na zagrożenia bezpieczeństwa w cyberprzestrzeni przez wszystkich użytkowników publicznie dostępnych systemów teleinformatycznych. Ustawodawca zasadnie dokonuje zatem wyodrębnienia dwóch grup podmiotów, tj. operatorów usług kluczowych oraz dostawców usług cyfrowych, na których spoczywa ciężar monitorowania cyberprzestrzeni oraz inicjowania działań zmierzających do neutralizowania zagrożeń i przywracania stanu bezpieczeństwa. W przekonaniu Autorów ustawodawca słusznie, idąc śladem prawodawcy unijnego (dyrektywa NIS), tworzy przestrzeń do współdziałania w zakresie realizacji tych obowiązków pomiędzy podmiotami świadczącymi usługi a organami państwa odpowiedzialnymi za zapewnienie bezpieczeństwa, obejmując je zbiorczą nazwą organów właściwych w zakresie cyberbezpieczeństwa.

Autorzy starają się przybliżyć nowe zagadnienia i odpowiedzieć na pytania, które zrodziły się w związku z zaproponowanymi przez ustawodawcę rozwiązaniami. Obok podstawowego celu, jaki przyświecał Autorom Komentarza sprowadzającego się do ustalenia zakresu i zasad stosowania zawartych w ustawie rozwiązań oraz skutków ich zastosowania, Autorzy prezentują także swój punkt widzenia na kwestie niedostatecznie jasno i jednoznacznie uregulowane w ustawie lub niekiedy pominięte, przez co dyskusyjne, budzące spory interpretacyjne, a więc wymagające dokonania wykładni przepisów ustawy, której efekty – w zamiarze Autorów – mogą stanowić wskazówkę w procesie ich stosowania.

Komentarz jest opracowaniem zbiorowym samodzielnych pracowników naukowych, dlatego objaśnienia pisane przez poszczególne osoby mają charakter autorski.

Zainteresowania badawcze Autorów wykraczają poza analizę prawną i obejmują problematykę właściwą dla nauk o bezpieczeństwie. Rozważania są zatem prowadzone w taki sposób, by z pola widzenia nie umknął zasadniczy cel regulacji, jakim jest zapewnienie bezpieczeństwa państwa (bezpieczeństwa narodowego). Autorzy wyrażają nadzieję, że zaproponowana szeroka perspektywa analizy stanowić będzie dodatkowy walor Komentarza.

Komentarz jest adresowany, przede wszystkim, do praktyków zajmujących się problematyką cyberbezpieczeństwa, w tym przedsiębiorców, prawników, a także studentów takich kierunków, jak: bezpieczeństwo narodowe, prawo, administracja, stosunki międzynarodowe. Na podział struktury treści Komentarza wpłynęła systematyka ustawy o krajowym systemie cyberbezpieczeństwa. Rozważania przypisane do każdej jednostki redakcyjnej zostały jednak podzielone także według wyodrębnionych zagadnień tematycznych, które zdaniem Autorów wymagały podkreślenia i zostały opatrzone krótkim tytułem sygnalizującym ich przedmiot. Dzięki takiemu zabiegowi edytorskiemu, w tym stosowanym wytłuszczeniom najistotniejszych tez do omawianych zagadnień, możliwe jest szybkie dotarcie do interesujących Czytelnika kwestii i uzyskanie odpowiedzi na napotykane problemy związane z wykładnią treści poszczególnych przepisów zawartych w ustawie. Komentarz do ustawy o krajowym systemie cyberbezpieczeństwa odnosi się do stanu prawnego na dzień 1.5.2019 r.

Dostrzegając znaczenie ochrony cyberprzestrzeni oraz wagę rozwiązań prawnych, które – w zamyśle ustawodawcy – powinny tę ochronę zapewnić, a zarazem mając na uwadze ciągły rozwój nowych technologii oraz nieustannie ewoluujące środowisko wirtualne, któremu dedykowane są zawarte w ustawie o krajowym systemie cyberbezpieczeństwa rozwiązania, Autorzy zakładają, że zawarte w Komentarzu ustalenia stanowić będą przyczynek do podjęcia dyskusji nad zaproponowaną wykładnią przepisów ustawy, jak również wskazane w nim uwagi zostaną uwzględnione w toku aktualizowania i modyfikowania instrumentów i narzędzi prawnych służących zapewnieniu bezpieczeństwa cyberprzestrzeni.

Autorzy