Streszczenie rozprawy doktorskiej

pt. „Krajowy System Cyberbezpieczeństwa”

Przedmiotem niniejszej pracy są zagadnienia dotyczące rozwiązań prawnych w obszarze cyberbezpieczeństwa, ze szczególnym uwzględnieniem ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Poruszana problematyka stanowi interesujący obszar badawczy, ze względu na znaczenie środków komunikacji elektronicznej oraz zastosowanie technologii informacyjno-komunikacyjnych w usługach kluczowych, usługach cyfrowych oraz w elektronicznej administracji. Przede wszystkim, analiza przedmiotowego zagadnienia pozwala na dokładne scharakteryzowanie katalogu zadań wyznaczonych przez ustawodawcę wobec konkretnych podmiotów administracji publicznej, operatorów usług kluczowych i dostawców usług cyfrowych. Przy czym należy wskazać, że głównym celem ustawodawcy jest zapewnienie cyberbezpieczeństwa świadczenia usług w kluczowych sektorach funkcjonowania państwa, również w aspekcie szacowania ryzyka i obsługi incydentów oraz zachowania poufności i integralności danych przetwarzanych w rejestrach elektronicznych.

Praca ma na celu przedstawienie przyjętych rozwiązań prawnych w kwestii cyberbezpieczeństwa, ukazanie ich zasadności oraz próbę oceny skuteczności przyjętych regulacji prawnych, zarówno w kontekście ustawy o krajowym systemie cyberbezpieczeństwa, jak i innych aktów prawnych odnoszących się do tej tematyki. Tezę wyjściową do przeprowadzanych badań wyraża stwierdzenie, iż współczesne zagrożenia bezpieczeństwa uzasadniają interdyscyplinarny charakter tego pojęcia. Uzasadnia to m.in. to, że krajowy system cyberbezpieczeństwa umożliwia wzmocnienie bezpieczeństwa systemów teleinformatycznych, usług kluczowych i usług cyfrowych, wpływając tym samym na bezpieczeństwo prawne, gospodarcze, społeczne i informatyczne w zakresie świadczonych usług. Kolejną tezą dysertacji jest to, że przyjmowane regulacje prawne w polskim porządku prawnym odzwierciedlają aktualne koncepcje i strategie bezpieczeństwa ustalone przez społeczność międzynarodową czy Unię Europejską. W przypadku ustawy o krajowym systemie cyberbezpieczeństwa, na jej kształt miała wpływ, w szczególności dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS).

Metody badawcze obejmują analizę aktów prawnych wraz z wykorzystaniem literatury przedmiotu. Metodologia pracy wyznaczona została przez założony cel, przy czym podstawową metodę badawczą wykorzystywaną w rozprawie stanowi metoda dogmatyczno-prawna uzupełniona o metodę prawno-porównawczą, oraz historyczno-prawną. Dokonano analizy przepisów zawartych w aktach prawa krajowego, prawa międzynarodowego, prawa unijnego, orzecznictwa i poglądów doktryny. Odwołano się do podstawowych regulacji prawnych w zakresie cyberbezpieczeństwa, przede

wszystkim do ustawy o krajowym systemie cyberbezpieczeństwa, ale także do ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawy o świadczeniu usług drogą elektroniczną, ustawy o usługach zaufania oraz identyfikacji elektronicznej, ustawy o dostępie do informacji publicznej, ustawy o ochronie danych osobowych. Analizie zostały poddane następujące akty prawa unijnego, m.in.: RODO, dyrektywa NIS, rozporządzenie eIDAS czy akt o cyberbezpieczeństwie oraz liczne koncepcje i strategie wypracowane zarówno przez społeczność unijną jak i międzynarodową. Ponadto, w pracy doktorskiej zaprezentowano koncepcje oraz stwierdzenia najwybitniejszych przedstawicieli doktryny, autorów pojęć i badaczy zagadnień związanych z cyberbezpieczeństwem. Przedstawiono także orzeczenia sądowe, w tym sądów administracyjnych, Trybunału Konstytucyjnego, instytucji unijnych.

Struktura pracy jest zgodna z przyjętymi tezami badawczymi oraz założeniami metodologii badawczej. Rozprawa doktorska, pt.: „Krajowy System Cyberbezpieczeństwa" obejmuje: wstęp, pięć rozdziałów merytorycznych (wraz z podrozdziałami), zakończenie (wnioski) i załączniki, które stanowią następujące materiały źródłowe: literatura przedmiotu, akty prawne, orzeczenia sądowe oraz inne źródła.

Mając na uwadze omówione w pracy konstrukcje prawne, można postawić tezę, że współczesne zagrożenia bezpieczeństwa uzasadniają interdyscyplinarny charakter tego pojęcia, a wskazanie zagrożeń pozwala na ustanowienie i zastosowanie przyjętych przepisów prawa. Bezpieczeństwo nie jest kategorią jednolitą i to nie tylko w znaczeniu terminologicznym. Za trafnością tego twierdzenia przemawiają wykazane liczne koncepcje bezpieczeństwa (prawne, gospodarcze czy technologiczne) oraz przepisy znajdujące się w aktach prawnych (w tym w Konstytucji RP i aktach szczególnego rodzaju). Współcześnie to cyberbezpieczeństwo stanowi podstawowy przedmiot zainteresowania prawa międzynarodowego i unijnego. Zapewnienie cyberbezpieczeństwa jest istotne w obrębie działań indywidualnych użytkowników sieci, instytucji, podmiotów administrujących które korzystają z e-usług.

Wynikiem przeprowadzonej w pracy analizy jest stwierdzenie, że obowiązująca ustawa o krajowym systemie cyberbezpieczeństwa konkretyzuje organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Można zatem stwierdzić, że stanowi wzorzec postępowania w przedmiotowym zakresie. De lege lata ustalono, że zasadność przyjętych regulacji odzwierciedla przede wszystkim opracowanie obowiązków poszczególnych podmiotów w odniesieniu do: wskazania rodzaju incydentów, ich klasyfikacji i obsługi, analizy ryzyka, obsługi i próby oceny szkód, jakie mogą wystąpić w związku z ich pojawieniem się w cyberprzestrzeni. Ustawa określa zadania właściwych podmiotów w strukturze krajowego systemu cyberbezpieczeństwa (operatorów usług kluczowych, dostawców usług cyfrowych i organów administracji publicznej). Uwzględniając zasygnalizowane w dysertacji problemy badawcze dotyczące

skuteczności wprowadzania powszechnie obowiązujących rozwiązań prawnych w trzech obszarach:
1) w ramach efektywnego i nieprzerwanego świadczenia usług kluczowych i usług cyfrowych;
2) bezpieczeństwa sieci, systemów teleinformatycznych oraz infrastruktury krytycznej,
3) przetwarzania danych osobowych i informacji niejawnych w elektronicznych zbiorach oraz określenia zasad identyfikacji elektronicznej, należy stwierdzić, że zarówno ustawa o krajowym systemie cyberbezpieczeństwa jak i inne akty prawne wymagają dostosowania przepisów do zmieniających się warunków technologicznych i społeczno-gospodarczych.

Ustawa o krajowym systemie cyberbezpieczeństwa może stanowić wzorzec postępowania dla elektronicznej administracji, tym samym pomóc w osiągnięciu wysokiego poziom bezpieczeństwa nie tylko w typowych usługach kluczowych czy cyfrowych ale wpłynąć całościowo na e-administrację. Określenie standardów cyberbezpieczeństwa jest szczególnie ważne, gdy daną usługę zakwalifikowano jako usługę kluczową czy usługę cyfrową. Tym bardziej, że coraz chętniej rozwiązania ICT wykorzystuje się w sektorze energii, finansów, transportu i ochrony zdrowia. Od wdrożenia inteligentnych technologii w dużej mierze zależy rozwój społeczno-gospodarczy oraz efektywne funkcjonowanie państwa.

Zasygnalizowane braki w unormowaniach prawnych pozwoliły na postawienie postulatów de lege ferenda odnoszących się do doprecyzowania i uaktualniania trzech zagadnień opisanych w ustawie o krajowym systemie cyberbezpieczeństwa. Po pierwsze w zakresie zagwarantowania aktualności Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej i partycypacji operatorów usług kluczowych, dostawców usług cyfrowych oraz specjalistów z dziedziny prawa komunikacji elektronicznej, czy nowych technologii, a także – fakultatywnie społeczeństwa w opracowaniu zasadniczej treści Strategii. Po drugie w materii dookreślenia i rozwinięcia treści protokołu i zaleceń pokontrolnych. Kolejno, można rozważyć wprowadzenie obowiązku posiadania przez operatorów usług kluczowych i dostawców usług cyfrowych określonej, aktualnej polityki cyberbezpieczeństwa świadczonych usług kluczowych i usług cyfrowych, ze szczególnym uwzględnieniem zasady zrównoważonego rozwoju, silnego uwierzytelnienia usługi i identyfikacji klienta w jej treści.

Temat niniejszej rozprawy ma znaczenie teoretyczne i praktyczne. Wnioski de lege ferenda mogą przyczynić się do ujęcia tematu cyberbezpieczeństwa w nowy sposób, mający na względzie aktualność rozwiązań ustawowych w odniesieniu do zmian technologicznych oraz prospołeczne znaczenie bezpieczeństwa cybernetycznego w kontekście dostępu do e-usług i powszechności informatyzacji. Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa wydaje się być nieunikniona. Co więcej, może spowodować również zmiany w innych powszechnie obowiązujących aktach prawnych w dziedzinie komunikacji elektronicznej czy informatyzacji administracji publicznej.

W pracy uwzględniono stan prawny obowiązujący na dzień 30 kwietnia 2020 r.