Wprowadzenie

Krajowy System Cyberbezpieczeństwa

Przejdź do produktu na **ksiegarnia.beck.pl**

Wprowadzenie

Współcześnie zagadnienia związane z tematyką bezpieczeństwa publicznego zajmują istotne miejsce w kontekście rozważań nad prawidłowym funkcjonowaniem państwa, świadczenia usług i rozwoju społeczno-gospodarczego. Jednakże błędem byłoby traktowanie bezpieczeństwa jedynie z punktu widzenia tradycyjnych metod i środków, których zastosowanie stanowi gwarancję jego zachowania. Wykorzystywanie narzędzi teleinformatycznych oraz popularyzacja środków komunikacji elektronicznej sprawiły, że pojęcie bezpieczeństwa nabrało innego **cybernetycznego** znaczenia.

W XXI w. na szeroką skalę przetwarza się dane osobowe i informacje niejawne w systemach teleinformatycznych, świadczy e-usługi w różnych dziedzinach życia publicznego, m.in. w sektorze finansowym czy energetycznym, czy prowadzi działania z zakresu zarządzania kryzysowego oraz obsługi infrastruktury krytycznej. Powyższe czyni zadość koncepcji społeczeństwa informacyjnego, czyli takiego, dla którego podstawową wartością jest dostęp do informacji. Komunikacja elektroniczna zaś w tym przypadku zapewnia co do zasady nieograniczony, powszechny przekaz informacji, możliwość załatwienia sprawy administracyjnej czy podjęcie działań społecznie użytecznych w łatwy i przystępny sposób. Bardzo ważna jest dostępność cyfrowa do stron internetowych oraz aplikacji mobilnych, którymi administrują podmioty publiczne[1]. Jednakże wszystko co podlega gromadzeniu w e-zbiorach czy jest realizowane poprzez e-usługi wymaga odpowiedniego zabezpieczenia przed zagrożeniami, mogącymi się pojawić w cyberprzestrzeni. Niestety, zagrożenia te mogą mieć zgoła różny charakter, w związku z czym zadania z zakresu cyberbezpieczeństwa są nad wyraz czasochłonne i wymagają wprowadzenia przejrzystych, aczkolwiek skutecznych reguł organizacyjno-prawnych.

Niniejsza praca ma na celu przedstawienie przyjętych rozwiązań prawnych w kwestii cyberbezpieczeństwa oraz ukazanie ich zasadności. Temat: **Krajowy system cyberbezpieczeństwa** jest niezwykle aktualny, ze względu na przyjętą w 2018 r. ustawę o tożsamym tytule[2] oraz istotny wobec zagrożeń bezpieczeństwa sieciowego. Cyberbezpieczeństwo jest zagadnieniem obecnym zarówno w krajowych, jak i ponadnarodowych dyskursach prawnych. Swoboda świadczenia usług i cyberbezpieczeństwo stanowią kluczowe zadania partnerów międzynarodowych, są przedmiotem spotkań bilate-

[1] *D. Sybilski*, Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych – kluczowe założenia, IAP 2019, Nr 2, s. 10–11.

[2] Ustawa z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r. poz. 913), dalej: CyberbezpU.

ralnych i multilateralnych, konferencji i paneli, zarówno w ramach kwestii faktycznych (przyjmowanie strategii działania), jak i dydaktycznych.

Kolejnym celem pracy jest próba oceny skuteczności przyjętych regulacji prawnych, zarówno w kontekście CyberbezpU, jak i innych aktów prawnych odnoszących się do tej tematyki. Uwzględniając interdyscyplinarny charakter bezpieczeństwa, podjęta zostanie analiza wprowadzonych przez organy administracji publicznej zmian i udoskonaleń obowiązujących przepisów, wynikająca z potrzeby bezpieczeństwa publicznego i wykluczenia bądź ograniczenia zagrożeń. Mając na uwadze zasadnicze cele pracy, głównym zadaniem badawczym będzie analiza i charakterystyka przepisów CyberbezpU i innych krajowych aktów prawnych istotnych w kontekście świadczenia usług drogą elektroniczną. Analizie zostaną poddane również regulacje unijne, takie jak: dyrektywa NIS[3], rozporządzenie eIDAS[4] czy RODO[5] i ich wpływ na przyjęte przez krajowego ustawodawcę akty powszechnie obowiązującego prawa. Podstawowym celem badawczym jest zatem analiza problematyki cyberbezpieczeństwa i zagadnień z nim związanych. Badania w zakresie poruszonej problematyki pozwolą wskazać potencjalne źródła zagrożeń dla prawidłowego funkcjonowania cyberprzestrzeni.

W opracowaniu scharakteryzowano katalog zadań wyznaczonych przez ustawodawcę wobec konkretnych podmiotów administracji publicznej, operatorów usług kluczowych i dostawców usług cyfrowych, istotnych na gruncie zapewnienia cyberbezpieczeństwa w ramach informatyzacji administracji czy świadczenia e-usług. Podkreślono, że cyberbezpieczeństwo powinno być traktowane w sposób całościowy, tj. obejmować wszystkie kluczowe dziedziny i sektory funkcjonowania państwa, a zatem usługi: cyfrowe, energetyczne, finansowe, transportowe czy zdrowotne, a także sektor prywatny. Przy czym należy wskazać, że o ile w sposób całkowity nie można ustrzec systemów teleinformatycznych przed zagrożeniami cybernetycznymi, o tyle możliwe jest przyjęcie określonych procedur w aspekcie szacowania ryzyka i obsługi incydentów. Najważniejsze zasady cyberbezpieczeństwa odnoszą się zatem do kwestii bezpieczeństwa systemowego, zachowania poufności i integralności danych oraz bieżącego monitorowa-

[3] 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 (Dz.Urz. UE L 194 z 19.7.2016 r., s. 1), dalej: dyrektywa NIS.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 28.8.2014 r., s. 73), dalej: eIDAS.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; Dz.Urz. UE L 119 z 4.5.2016 r., s. 1), dalej: RODO.

nia odporności systemów[6]. Zaangażowanie krajowych struktur cyberbezpieczeństwa należy odczytywać także na płaszczyźnie współdziałania z organami Unii Europejskiej (dalej: UE), Organizacji Traktatu Północnoatlantyckiego (dalej: NATO), innymi organami i instytucjami o charakterze międzynarodowym.

Mając na uwadze zarówno powszechny, jak i indywidualny wymiar cyberbezpieczeństwa oraz celowość przyjętych metod ochrony, zidentyfikowano podstawowe zasady cyberbezpieczeństwa (poufności, integralności i dostępności danych, ochrony infrastruktury krytycznej), w tym bezpieczeństwa elektronicznego oraz scharakteryzowano współczesne zagrożenia cyberbezpieczeństwa (cyberprzestępczość czy cyberterroryzm). Opracowanie zawiera charakterystykę rozwiązań prawnych przyjętych wobec następujących terminów teoretycznych: bezpieczeństwo, cyberprzestępczość, cyberterroryzm, cyberbezpieczeństwo, e-administracja, usługi cyfrowe i usługi kluczowe, władztwo administracyjne organów w walce z zagrożeniami bezpieczeństwa. Zasadnicze problemy badawcze przedmiotowej pracy dot. kwestii 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.

Oprócz zagadnień ściśle dot. założeń krajowego systemu cyberbezpieczeństwa, przeprowadzona analiza pozwoli na zbadanie problematyki bezpieczeństwa elektronicznego w obrębie usług świadczonych przez e-administrację, w tym możliwość zastosowania przepisów CyberbezpU w typowych dla administracji elektronicznej zadaniach.

Nie ulega wątpliwości, że współczesne zagrożenia bezpieczeństwa uzasadniają interdyscyplinarny charakter tego pojęcia. Co więcej, stan bezpieczeństwa państwa w dziedzinie finansów, gospodarki, obrony, cybernetyki i innych, zależy od przeprowadzenia wstępnej procedury kwalifikacyjnej istniejących zagrożeń, której skutkiem jest stanowienie i stosowanie przyjętych przepisów prawa. Krajowy system cyberbezpieczeństwa umożliwia wzmocnienie bezpieczeństwa systemów teleinformatycznych, usług kluczowych i usług cyfrowych oraz głównych zadań państwa (zadań z zakresu użyteczności publicznej). Zaznaczyć należy, że pierwszoplanową rolę pełnią jednostki ministerialne (rząd), ich reakcja na zaistniałe incydenty powoduje sekwencję kolejnych zdarzeń w bezpośredniej neutralizacji zagrożenia. Nieoceniona jest także postawa operatorów usług kluczowych i dostawców usług cyfrowych w zakresie dokonywania kontroli, zapewnienia ciągłego świadczenia e-usług oraz obsługi i klasyfikacji incydentu

[6] *M. Kruk*, Obowiązki dostawców usług cyfrowych na gruncie ustawy o krajowym systemie cyberbezpieczeństwa jako element poprawy bezpieczeństwa w świecie cyfrowym oraz przeciwdziałaniu cyberprzestępstwom, PME 2019, Nr 1, s. 28.

sieciowego. Przyjmowane w polskim porządku prawnym regulacje prawne odzwierciedlają aktualne koncepcje i strategie ustalone przez społeczność międzynarodową czy UE. W przypadku CyberbezpU na jej kształt miała wpływ w szczególności dyrektywa NIS.

Uzasadnienie powyżej wskazanych tez wymagało przeprowadzenia kompleksowej analizy aktów prawnych o tematyce cyberbezpieczeństwa, prawa krajowego, unijnego i międzynarodowego oraz klasyfikacji poszczególnych pojęć i terminów z zakresu technologii informacyjno-komunikacyjnych (dalej: ICT) odnoszących się do tematyki cyberbezpieczeństwa. Metody badawcze obejmują analizę aktów prawnych wraz z wykorzystaniem literatury przedmiotu. Podstawową metodę badawczą stanowi metoda dogmatyczno-prawna. Metoda ta została uzupełniona o metodę prawno-porównawczą oraz historyczno-prawną.

W przypadku metody dogmatyczno-prawnej 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 CyberbezpU, ale także do m.in. ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[7], ustawy o świadczeniu usług drogą elektroniczną[8], ustawy o usługach zaufania oraz identyfikacji elektronicznej[9]. Analizie zostały poddane następujące akty prawa unijnego, m.in.: RODO, dyrektywa NIS, eIDAS czy akt o cyberbezpieczeństwie[10] oraz liczne koncepcje i strategie wypracowane zarówno przez społeczność unijną, jak i międzynarodową. Ponadto w pracy zaprezentowano koncepcje oraz stwierdzenia najwybitniejszych przedstawicieli doktryny, autorów pojęć i badaczy zagadnień związanych z cyberbezpieczeństwem. Przedstawiono orzeczenia sądowe, w tym sądów administracyjnych, Trybunału Konstytucyjnego (dalej: TK), instytucji unijnych. Pomocniczo wykorzystano również aktualne informacje i wykazy zamieszczone na stronach internetowych właściwych instytucji, ministerstw, organów krajowych i międzynarodowych. W celu rozwiązania problemów badawczych i udowodnienia postawionych w pracy tez posłużono się źródłami prawa administracyjnego, prawa komunikacji elektronicznej, prawa gospodarczego, prawa finansowego, prawa karnego, prawa cywilnego, prawa unijnego.

W ramach metody prawno-porównawczej pozyskana literatura oraz dostępność powszechnie obowiązujących aktów prawa pozwoliły na porównanie krajowych roz-

---

[7] Ustawa z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r. poz. 57), dalej: InformPodPublU.

[8] Ustawa z 18.7.2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344), dalej: ŚwiadUsłElektU.

[9] Ustawa z 5.9.2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r. poz. 1797), dalej: UsłZaufU.

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.4.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) Nr 526/2013 (akt o cyberbezpieczeństwie; Dz.Urz. UE L 151 z 7.6.2019 r., s. 15).

wiązań (zawartych w ustawach czy rozporządzeniach) z regulacjami prawa unijnego oraz prawa międzynarodowego. Z kolei metoda historyczno-prawna umożliwiła wskazanie zmian w przepisach prawa krajowego w kwestii bezpieczeństwa cyberprzestrzeni, przede wszystkim organizacyjno-prawnych, ale także gospodarczych, społecznych i technologicznych. Pozwoliła również przedstawić różnorodność rozważań doktrynalnych i filozoficznych w odniesieniu do próby zdefiniowania bezpieczeństwa, zasad demokratycznego państwa prawnego i sprawiedliwości społecznej.

Komparatystyczna analiza tekstów aktów prawnych, wraz z wykorzystaniem literatury przedmiotu, orzeczeń sądowych, poglądów doktryny, przeprowadzona na podstawie następujących metodyk badań: dogmatyczno-prawnej, prawno-porównawczej i historyczno-prawnej, umożliwiła sformułowanie w poszczególnych rozdziałach pracy oraz zakończeniu wniosków *de lege lata* i *de lege ferenda.*

Na układ pracy wpływ miały podstawowe cele i założenia badawcze. Struktura pracy jest zgodna z przyjętymi tezami badawczymi i założeniami metodologii badawczej. Praca obejmuje: wstęp, pięć rozdziałów merytorycznych (wraz z podrozdziałami), zakończenie i materiały źródłowe: literaturę przedmiotu, akty prawne, orzeczenia sądowe oraz inne źródła.

W pierwszym rozdziale pracy, zatytułowanym: **Bezpieczeństwo jako element prawidłowego funkcjonowania państwa**, przedstawiono zagadnienia związane z określeniem znaczenia bezpieczeństwa w demokratycznym państwie prawnym. Bezpieczeństwo, według rozważań zawartych w przedmiotowym rozdziale, stanowi dobro wspólne całego narodu, naczelną wartość pozostającą pod ochroną państwa polskiego, w tym Konstytucji Rzeczypospolitej Polskiej[11] oraz aktów prawa międzynarodowego. Ponadto w rozdziale I określono: definicje i różne rodzaje oraz koncepcje bezpieczeństwa, i jego współczesne zagrożenia. Analizie poddano także: znaczenie decentralizacji w kontekście bezpieczeństwa demokratycznego państwa prawnego, zasady bezpieczeństwa prawnego, bezpieczeństwa gospodarczego, bezpieczeństwa wewnętrznego i zewnętrznego w ramach porządku publicznego, aspekty bezpieczeństwa w prawie międzynarodowym oraz kwestie bezpieczeństwa informatycznego i technologicznego.

Rozdział II, zatytułowany: **Założenia krajowego systemu cyberbezpieczeństwa**, obejmuje dokładną charakterystykę treści przepisów zawartych w CyberbezpU. Uwzględniono w nim najważniejsze kwestie dot.: identyfikacji oraz wykazu operatorów usług kluczowych i dostawców usług cyfrowych oraz ich zadania, a także obowiązki właściwych organów w sferze cyberbezpieczeństwa czynności z zakresu kontroli i nadzoru. Poruszone zostało również zagadnienie wpływu regulacji zarówno prawa unijnego, jak i pozostałych aktów prawa krajowego, na krajowy system cyberbezpieczeństwa. W tym znaczeniu analizie poddano unijne aspekty cyberbezpieczeństwa zawarte w: eIDAS, dyrektywie NIS, akcie o cyberbezpieczeństwie. Wskazano w nim pewne postulaty zmian przepisów CyberbezpU co do określenia treści protokołu kontroli,

[11] Konstytucja Rzeczypospolitej Polskiej z 2.4.1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.), dalej: Konst.

w przypadku stwierdzenia nieprawidłowości w zakresie obsługi incydentu oraz treści zaleceń pokontrolnych dot. usunięcia nieprawidłowości.

W rozdziale III, pt. **Cyberbezpieczeństwo i bezpieczeństwo sieciowe**, analizie poddano następujące aspekty: cyberbezpieczeństwo powszechne i indywidualne oraz rodzaje zagrożeń bezpieczeństwa sieciowego (w tym przestępczość internetową i cyberterroryzm), pod kątem określenia zasad i zadań organów administracji publicznej podejmowanych w celu wykrycia i zneutralizowania zagrożenia. Szczególną uwagę zwrócono na rozwiązania w zakresie wskazania strategicznych celów i priorytetów cyberbezpieczeństwa w strategii cyberbezpieczeństwa. Wskazano zasadność opracowania zmian w CyberbezpU w zakresie zasad wprowadzania strategii cyberbezpieczeństwa.

Rozdział IV, pt. **Bezpieczeństwo sektorowe**, zawiera opis obowiązków organów, właściwych instytucji i podmiotów w celu nieprzerwanego i wydajnego świadczenia usług o kluczowym znaczeniu dla społeczeństwa, takich jak usługi: cyfrowe, energetyczne, finansowe, transportowe i zdrowotne. Obejmuje opis metod zarządzania, ze względu na wykorzystywanie technologii informacyjnej w ich świadczeniu. W rozdziale wskazano możliwości zastosowania innowacyjnych rozwiązań teleinformatycznych, takich jak np. smart city, cloud computing czy GPS w istotnych dla rozwoju społeczno-gospodarczego sektorach usług publicznych. Analiza zagadnień pozwoli na przyjęcie postulatów *de lege ferenda* w przedmiocie stworzenia efektywnego, skutecznego i bezpiecznego kanału dystrybucji określonej usługi, poprzez wskazanie wprowadzenia odpowiednich przepisów do CyberbezpU w zakresie wdrożenia określonej polityki cyberbezpieczeństwa świadczonych usług kluczowych i usług cyfrowych.

W rozdziale V, pt. **Bezpieczeństwo elektroniczne w administracji**, omówiono najważniejsze koncepcje i zasady prawa administracyjnego, mające ogromny wpływ na realizację zadań publicznych, tak w wymiarze tradycyjnym, jak i elektronicznym. Poddano analizie pojęcie władztwa administracyjnego organów administracji publicznej. Ponadto przedstawiono istotne funkcje e-administracji, usługi administracji publicznej świadczone drogą elektroniczną, standardy bezpieczeństwa elektronicznego w administracji oraz znaczenie społeczeństwa informacyjnego i prawa do dobrej administracji w kontekście możliwości zastosowania ICT w administracji publicznej. Określono także możliwość zastosowania regulacji zawartych w CyberbezpU w świadczeniu usług przez e-administrację.

Niniejsza praca w efekcie powinna określić, czy cel CyberbezpU, jakim było zapewnienie cyberbezpieczeństwa usług kluczowych i usług cyfrowych, a także cele innych aktów prawnych traktujących o bezpieczeństwie mogą być kompleksowo zrealizowane w dobie zagrożeń cyberprzestrzeni. Po drugie, czy organy administracji publicznej są w stanie przewidzieć przyczyny i skutki takich zagrożeń i właściwie reagować, gdy się już pojawią. Kolejno, czy wprowadzone regulacje prawne wymagają udoskonalenia, czy też w pełni rozwiązują problem zagrożeń cybernetycznych. Liczba publikacji odnosząca się do tematu cyberbezpieczeństwa co prawda wzrasta, ale nadal brakuje w niej odniesień do kluczowych elementów bezpieczeństwa sieciowego; być może niniejsza praca choćby częściowo umożliwi zrozumienie koncepcji bezpieczeństwa cybernetycznego

i zasady jego ochrony. Wnioski *de lege lata* i postulaty *de lege ferenda* przedstawione w poszczególnych rozdziałach monografii pozwolą na kompleksowe sformułowanie wniosków końcowych, wskazanych w zakończeniu. Praca objęła stan prawny na dzień 1 czerwca 2023 r.

Podziękowania

Składam szczególne podziękowania Promotor, Pani dr hab. prof. US *Aleksandrze Monarcha-Matlak* za nieocenione wsparcie podczas przygotowywania niniejszej pracy, ale również za wiele cennych wskazówek w sprawach naukowych, zawodowych, całą przekazaną wiedzę oraz okazaną życzliwość.

Pragnę także podziękować koleżankom i kolegom z Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego za inspirujące rozmowy oraz wsparcie naukowe.

Dziękuję również moim bliskim – rodzinie i przyjaciołom, za dobre słowo i wsparcie oraz motywację do działania.

Szczecin, czerwiec 2023 r.

Dominika Skoczylas

Przejdź do księgarni ➜

C.H.BECK ksiegarnia.beck.pl