SEKRETARIAT DZIEKANA
WPiA US
10.03.2021
1.dz. 826/2021
WPŁYNĘŁO

Warszawa, 25.02.2021 r.

Prof. dr hab. Grażyna Szpor,
Kierownik Katedry Prawa Informatycznego
UKSW w Warszawie

Recenzja rozprawy doktorskiej Pani magister Dominiki Skoczylas
„Krajowy system cyberbezpieczeństwa"

1. Uwagi ogólne

Niniejsza opinia sporządzona została w związku z uchwałą Rady Naukowej Instytutu Nauk Prawnych Uniwersytetu Szczecińskiego z dnia 20 listopada 2020 r. o powierzeniu mi - zgodnie z art.20 ust. 5 i 6 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniu i tytułach w zakresie sztuki (tekst jedn. Dz. U. z 2017 r. poz. 1789) w związku z art. 179 ustawy z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1669 z późn. zm.) - funkcji recenzenta w przewodzie doktorskim Pani magister Dominiki Skoczylas. Jej rozprawa doktorska „Krajowy system cyberbezpieczeństwa", napisana została pod kierunkiem Pani prof. US dr. hab. Aleksandry Monarchy-Matlak jako promotora i doktora Przemysława Zdyba jako promotora pomocniczego.

Przedmiotem recenzji jest w szczególności ustalenie, czy otrzymana rozprawa doktorska spełnia wymogi określone w art. 13. przywołanej wyżej ustawy z dnia 14 marca 2003 r. Według tego przepisu, przygotowywana pod opieką promotora rozprawa powinna: stanowić oryginalne rozwiązanie problemu naukowego, wykazywać ogólną wiedzę teoretyczną kandydata w danej dyscyplinie naukowej oraz umiejętność samodzielnego prowadzenia pracy naukowej.

Jurydyzacja ochrony przed zagrożeniami związanymi z rozległymi sieciami komputerowymi postępuje od półwiecza, ale dopiero od kilku lat pojawiają się bardziej kompleksowe unijne i krajowe akty z tego zakresu. Krytykowanym, lecz użytecznym i nie

mającym atrakcyjnej alternatywy terminem zbiorczym, staje się w języku prawnym i prawniczym „cyberbezpieczeństwo". Kontrowersyjność jego znaczenia sprawia, że nadany rozprawie tytuł tożsamy z tytułem wiodącej polskiej ustawy ma charakter problemowy.

We wstępie wskazuje się jako cele badań: analizę i charakterystykę regulacji oraz próbę oceny skuteczności przyjętych rozwiązań przez pryzmat: 1. efektywnego i nieprzerwanego świadczenia usług kluczowych i usług cyfrowych 2. Bezpieczeństwa sieci i systemów teleinformatycznych oraz infrastruktury krytycznej 3. Przetwarzania danych osobowych i informacji niejawnych w elektronicznych zbiorach oraz określenia zasad identyfikacji elektronicznej [s.9-11].

Zarówno to, że badane są nowe akty prawne nie mające jeszcze wyczerpującej doktrynalnej wykładni, jak i oryginalna koncepcja trójelementowej weryfikacji skuteczności regulacji, stwarzają możliwość wypełnienia istotnej luki poznawczej. Natomiast założone określenie „potencjalnych źródeł zagrożeń dla prawidłowego funkcjonowania cyberprzestrzeni" rysuje perspektywę praktycznej przydatności poczynionych w rozprawie ustaleń.

Oceniając przedstawiony problem naukowy jako aktualny i istotny, rozważyć należy najpierw oryginalność jego rozwiązania a następnie także spełnienie pozostałych wymogów ustawowych.

2. Oryginalne rozwiązanie problemu naukowego

Wyniki badań krajowego systemu cyberbezpieczeństwa, przedstawiono w liczącej 453 strony rozprawie obejmującej „Wprowadzenie" [s.9-16], 5 rozdziałów i „Zakończenie" [s. 368-386] a ponadto zawierającej wykaz cytowanych publikacji [s. 387-445] i streszczenia [446-453]. Konstrukcja rozprawy jest przejrzysta, podział proporcjonalny a treść poszczególnych rozdziałów - zaczynających się uwagami wstępnymi a kończących konkluzjami - adekwatna do ich tytułów.

Weryfikowane są tezy, że „współczesne zagrożenia bezpieczeństwa uzasadniają interdyscyplinarny charakter pojęcia", krajowy system cyberbezpieczeństwa umożliwia wzmacnianie bezpieczeństwa systemów teleinformatycznych, usług kluczowych, usług cyfrowych i całego państwa a krajowe regulacje prawne odzwierciedlają aktualne strategie międzynarodowe i unijne [s.11,12].

W rozdziale pierwszym ukazane zostało bezpieczeństwo jako element prawidłowego funkcjonowania państwa" [s.17-77], a w szczególności jako fundament demokratycznego państwa prawnego [pkt 2.]. Uwzględniono bezpieczeństwo międzynarodowe oraz krajowe - zewnętrzne i wewnętrzne a także bezpieczeństwo: prawne, gospodarcze, informatyczne i technologiczne. Zestawiono również jego filozoficzne koncepcje, definicje i „rodzaje" [p.3.] Doktorantka prezentuje pogłębioną, interdyscyplinarną analizę bezpieczeństwa, której wycinkiem, jednym z rodzajów, jest cyberbezpieczeństwo. Jednak w tym miejscu [s.64] należało mu poświęcić więcej miejsca, bo rozproszenie objaśnień tego kluczowego terminu prawnego w kilku rozdziałach utrudnia recepcję. Ponadto używanie jako synonimu określenia „bezpieczeństwo cybernetyczne", choć w świetle urzędowego przekładu unijnych aktów dopuszczalne, jest w literaturze oceniane krytycznie – do czego należało się odnieść. W prezentacji współczesnych zagrożeń [p.4.] docenić należy rozważania o znaczeniu decentralizacji dla bezpieczeństwa państwa, których wagę potęgują polskie doświadczenia czasu pandemii. Zwraca też uwagę rozpatrywanie bezpieczeństwa prawnego w kontekście „zadań władzy sądowniczej" [pkt. 3.2].

Rozdział 2. charakteryzuje założenia krajowego systemu cyberbezpieczeństwa, najpierw na tle międzynarodowej i unijnej regulacji a potem krajowego otoczenia prawnego. W pierwszej części nieoczywiste, ale wzbogacające ogląd, jest uwzględnienie poza dyrektywą NIS [bez przywołania europejskiej strategii cyberbezpieczeństwa z 2013 r.] i rozporządzeniem PEiR 2019/881 - także rozporządzenia eIDAS. W części drugiej zwięźle a obrazowo ukazywane są fakty motywujące do wzmacniania ochrony prawnej [s. 101-103], szerzej analizowane w rozdziale następnym. W punkcie 3.1. zatytułowanym „Ustawa o Krajowym Systemie Cyberbezpieczeństwa" [s. 104-121] referowane są poglądy wielu autorów wyrażane w licznych aktualnych publikacjach. Zapewne przyczyniło się to do kontrowersyjnych ujęć: relacji między dyrektywą NIS a ustawą o ksc i nazywania samej ustawy strategią [s.105], czy - wykraczającego poza wymogi dyrektywy - miejsca podmiotów sektora finansów publicznych wśród podmiotów krajowego systemu cyberbezpieczeństwa [s. 107, 117]. W obszernym podsumowaniu rozdziału [s. 150 - 152] Doktorantka charakteryzując założenia krajowego systemu cyberbezpieczeństwa trafnie eksponuje znaczenie wielopoziomowości regulacji a szczególnie prawa unijnego. Należy się też zgodzić, że ze względu na transgraniczny charakter świadczenia usług kluczowych i usług cyfrowych, istotne stało się jednoczesne zacieśnienie współpracy w zakresie cyberbezpieczeństwa w ramach e-usług i cyberobrony. Pozytywna

ocena starań o ujednolicenie regulacji prawnych we wszystkich państwach członkowskich, „co do tak ważnych zadań jak: identyfikacja elektroniczna i usługi zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS), bezpieczeństwo sieci i systemów teleinformatycznych na terytorium Unii (dyrektywa NIS), ochrona danych osobowych osób fizycznych, przetwarzanie i swobodny przepływ danych osobowych (RODO), certyfikacja cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie)", prowadzi Doktorantkę do istotnego wniosku. Wprawdzie warto było odnieść się w nim do znaczenia nadawanego cyberbezpieczeństwu w prawnych definicjach, ale w sferach badań, legislacji i realizowania prawa rzeczywiście należy je „traktować bardzo szeroko, zarówno przez pryzmat bezpieczeństwa e-usług i e-transakcji, zastosowania odpowiednich i optymalnych rozwiązań informatycznych i teleinformatycznych w procesie przetwarzania informacji i dostarczania usług, oraz w materii bezpiecznego przetwarzania danych osobowych" - a wiele podmiotów systemu jeszcze sobie tego nie uświadamia. Dodatkowo pojawia się tu także postulat konkretnego „doregulowania" w polskiej ustawie kontroli i nadzoru nad operatorami usług kluczowych i dostawcami usług cyfrowych, wpisujący się w ogólną tendencję badań skuteczności prawa, w których nota bene pojawiała się też koncepcja jednorazowego unormowania tych kwestii [np. w ustawie o NIK] i zamieszczania w innych aktach tylko przepisu odsyłającego.

W rozdziale 3. „Cyberbezpieczeństwo i bezpieczeństwo sieciowe" [s.153 - 201] obszernie charakteryzowane jest cyberbezpieczeństwo powszechne i indywidualne [s.154 - 166] a następnie rodzaje zagrożeń bezpieczeństwa sieciowego [pkt. 3], przestępczość internetowa [pkt. 3.1.] i cyberterroryzm [3.2]. W podsumowaniu [s.199 – 201] zwraca się uwagę, że „zapewnienie cyberbezpieczeństwa jest istotne zarówno w obrębie działań indywidualnych użytkowników sieci, jak i określonych grup, instytucji, podmiotów administrujących które korzystają z e-usług (np. z chmury obliczeniowej)", co nadaje wysoką rangę opracowaniu standardów bezpieczeństwa cyfrowego, oraz wskazaniu organów właściwych odpowiedzialnych za ich wdrożenie. Przy pozytywnej ocenie przez Doktorantkę samego zawarcia w ustawie o krajowym systemie cyberbezpieczeństwa obowiązku opracowania Strategii Bezpieczeństwa Rzeczpospolitej Polskiej, w rozdziale formułowane są też uwagi krytyczne. Dotyczą one nie zapewniania aktualności i aktualizacji strategii ani partycypacji w kształtowaniu jej treści operatorów usług kluczowych, dostawców usług cyfrowych i specjalistów z „dziedziny prawa komunikacji elektronicznej, czy nowych

technologii", a także konsultacji społecznych, gdy „obostrzenia prawne, w istotny sposób ograniczałyby prawa i wolności obywatelskie" [s.200]. Realizację zawartego w recenzowanej rozprawie postulatu dookreślenia przepisów dotyczących wdrażania strategii cyberbezpieczeństwa, aktualizacji i partycypacji, przekonująco uzasadnia zarysowana perspektywa uwzględniania dzięki temu w strategiach zarówno zmian technicznych i technologicznych jak i potrzeb społeczeństwa informacyjnego wynikających z intensyfikacji działań cyberprzestępczych i terrorystycznych [s.201].

W rozdziale 4. dotyczącym „bezpieczeństwa sektorowego" [s.202-255] analizowane są kolejno usługi: cyfrowe [s. 203 – 221], energetyczne [s.222 229], finansowe [s.230 -237], transportowe [238-245] oraz zdrowotne [s.246-252]. Konkluzje [s.253-255] pokazują umiejętność syntetycznego ujmowania przez Doktorantkę rozległych i skomplikowanych zagadnień, zorientowanego na sformułowanie i logicznie poprawne uzasadnienie postulatów zmian regulacji. Należy też docenić ambitne próby konkretyzacji proponowanych nowych przepisów ustawy o krajowym systemie cyberbezpieczeństwa, wprowadzenia: „art. 10. ust. 1a, w brzmieniu: „Operator usługi kluczowej opracowuje politykę cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, uwzględniając: a) silne uwierzytelnienie usługi i identyfikację użytkownika, b) innowacyjność i interoperacyjność usługi kluczowej, c) zasadę zrównoważonego rozwoju." oraz „art. 17 ust. 3a, w brzmieniu: „Dostawca usługi cyfrowej w celu zapewnienia ciągłości świadczenia usługi opracowuje politykę cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi cyfrowej, uwzględniając: a) silne uwierzytelnienie usługi i identyfikację użytkownika, b) innowacyjność i interoperacyjność usługi cyfrowej, c) zasadę zrównoważonego rozwoju". Poczynione ustalenia dobrze świadczą zarówno o intuicji badawczej mgr Dominiki Skoczylas jak i umiejętności jej spożytkowania.

Najobszerniejszy w rozprawie rozdział 5. [s. 256-367] koncentruje się na „bezpieczeństwie elektronicznym w administracji", uwzględniając problemy władztwa administracyjnego organów administracji publicznej [s. 257-276] oraz funkcje e-administracji [s. 277-347], przy czym tytuł punktu 4. [s. 348-364] powinien mieć inne brzmienie niż tytuł rozdziału, którego jest częścią. Analiza tych zagadnień prowadzi Doktorantkę do konkluzji, że „określenie polityki cyberbezpieczeństwa w kwestii usług świadczonych przez elektroniczną administrację jest równie ważne jak wskazanie obowiązków operatorów usług kluczowych czy dostawców usług kluczowych" a przysługujące organom administracji publicznej władztwo

administracyjne w przypadku cyberbezpieczeństwa „może być skutecznym narzędziem umożliwiającym natychmiastową reakcję, gdy bezpieczeństwo przekazu informacji czy świadczenia usługi na odległość jest zagrożone". Autorka ocenia, że „w kontekście e-administracji, z aprobatą należy przyjąć atrybuty władztwa administracyjnego", bowiem „Podjęcie zdecydowanych działań w przypadku wystąpienia incydentu, może uchronić system przed negatywnymi skutkami cyberzagrożenia i zapewnić niezakłócone świadczenie usługi". Równocześnie podkreśla jednak, że e-administracja, wykorzystuje technologie informacyjno-komunikacyjne w celu uproszczenia struktur organizacyjnych w sferze wewnętrznej i zewnętrznej, a w zakresie załatwiania sprawy urzędowej on-line podstawowe znaczenie ma dostępność oraz użyteczność informacji czy usługi dla użytkownika platformy zarządzanej przez właściwe organy administracji elektronicznej, toteż „e-administracja oprócz realizacji zasad wynikających z tzw. prawa do dobrej administracji musi mieć na względzie transparentność, skuteczność i bezpieczeństwo przekazu" [s. 365]. Te trafne ustalenia dotyczące władczych i niewładczych form działania kończy kontrowersyjne stwierdzenie, że „współcześnie, funkcje e-administracji, takie jak: informacyjna, integracyjna, interakcyjna, konsultacyjna, transakcyjna, czy ochronna muszą być zorientowane na świadczenie usług użyteczności publicznej" [s. 356], a bardzo skrótowe potraktowanie w rozprawie interdyscyplinarnego problemu funkcji administracji [s. 315, 316] nie pozwala go lepiej zrozumieć. Interdyscyplinarna perspektywa pojawia się natomiast w omawianym rozdziale w ujęciu jako przejawu jurydyzacji „elektronicznego zarządzania" aktów, które wyznaczają warunki właściwego wykorzystania ICT w e-administracji i e-usługach i własne zestawienie najważniejszych spośród nich. Godne uwagi jest także zestawienie pozytywnie ocenianych przez Doktorantkę przejawów wykorzystania nowych technologii w celu realizacji zadań społecznie użytecznych. Rzeczywiście stanowią one „kamienie milowe" w rozwoju społeczeństwa informacyjnego, także gdy rozpatrujemy je przez pryzmat funkcji obejmujących - w świetle socjologii administracji – zarówno to, co normatywnie postulowane jak i to, co realnie obserwowane. Kwestią, która przewija się w całej rozprawie jest wielość zadań podmiotów administrujących i złożoność ich wzajemnych relacji w krajowym systemie cyberbezpieczeństwa, zebrana na końcu ostatniego rozdziału [s. 366, 367]. Jednak klarowność wywodu zwiększyłoby zapewne syntetyczne scharakteryzowanie regulacji dotyczącej statusu podmiotów sektora finansów publicznych w ustawie o krajowym systemie cyberbezpieczeństwa na początku pracy.

„Zakończenie" rozprawy zawiera podsumowanie ustaleń poczynionych w poszczególnych rozdziałach w kontekście weryfikowanej tezy, że „współczesne zagrożenia cyberbezpieczeństwa uzasadniają interdyscyplinarny charakter tego pojęcia" [s. 11,12], w tym krytyczne uwagi de lege lata. W szczególności zwraca uwagę wniosek, że „skuteczność wprowadzania powszechnie obowiązujących rozwiązań prawnych wymaga określenia takich przepisów, które zapewnią: efektywne i nieprzerwane świadczenie usług kluczowych i usług cyfrowych, bezpieczeństwo sieci, systemów teleinformatycznych, infrastruktury krytycznej, oraz określą zasady przetwarzania danych osobowych i informacji niejawnych w elektronicznych zbiorach i zasady identyfikacji elektronicznej". Przez pryzmat tej konstatacji należy rozpatrywać prezentowane następnie zbiorczo postulaty de lege ferenda odnoszące się do strategii cyberbezpieczeństwa oraz kontroli i nadzoru. Ponadto w zakończeniu sygnalizowane jest rozpoczęcie prac nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, w których te uwagi i postulaty mogą być brane pod uwagę.

Niewątpliwie wiedza Doktorantki powinna być nie tylko w tym ale i w innych równolegle toczących się procesach legislacyjnych wykorzystana. Rośnie świadomość, że sterowanie aktywnością w cyberprzestrzeni nie może obywać się bez pieczy podmiotów publicznych jako regulatorów. Przy obecnej segmentacji problemu bezpieczeństwa w Internecie i normowaniu poszczególnych segmentów aktem wiodącym i przepisami rozproszonymi w wielu innych aktach, systemowe ujmowanie celu regulacji i operacji uznawanych za niezbędne dla jego osiągnięcia, uważam za istotny aspekt modelowania skuteczności prawa informatycznego. Dlatego wpisującą się w ten nowy nurt badań rozprawę Pani mgr Dominiki Skoczylas oceniam jako zasługujące na wyróżnienie, oryginalne rozwiązanie problemu naukowego polegające na ukazaniu znaczenia pojmowania cyberbezpieczeństwa dla skuteczności regulacji prawnej.

3. Ogólna wiedza teoretyczna Kandydata w dyscyplinie naukowej

Wiedzę teoretyczną Doktorantki pokazuje dobór i sposób wykorzystania źródeł. W końcowym ich wykazie znalazło się 48 krajowych aktów prawnych oraz 26 międzynarodowych i unijnych, 27 orzeczeń sądów i trybunałów, aż 397 pozycji krajowej i zagranicznej literatury a także około 100 pozycji źródłowych nie mieszczących się w wymienionych kategoriach.

Ogólną znajomość literatury prawniczej z szerokiego zakresu objętego tematyką pracy oceniam jako bardzo dobrą, odnotowując przy tym racjonalne przywoływanie publikacji zagranicznych, zwłaszcza artykułów opublikowanych w ostatnich latach w kilku anglojęzycznych czasopismach naukowych. Niewątpliwym utrudnieniem w realizacji celów badawczych było interdyscyplinarne podejście, wymagające zapoznania się z ustaleniami poczynionymi na gruncie nauk pozaprawnych, z czym Doktorantka dobrze sobie - z nielicznymi wyjątkami - poradziła.

Sprawnie referowane są w rozprawie przepisy prawne, zawarte w bardzo wielu obowiązujących aktach wielopoziomowej regulacji . Można jednak zauważyć, że Doktorantka wgłębiwszy się w badaną materię, niektóre podstawowe i szeroko już wcześniej komentowane w literaturze przepisy tylko lapidarnie kwituje w odsyłaczach, co dotyczy też definicji prawnych cyberbezpieczeństwa. O ile w pracy doktorskiej jest to akceptowalne, to dla potrzeb publikacji książkowej wymagałoby rewizji. Natomiast dokonywana wykładnia przepisów tylko sporadycznie skłania do polemiki.

Bardzo solidne podstawy źródłowe rozprawy znajdują odzwierciedlenie w 847 prawidłowo zredagowanych przypisach, zawierających przede wszystkim skrupulatne odesłania do referowanych poglądów innych autorów a w niezbędnym zakresie także orzecznictwo, akty prawne i dokumenty urzędowe oraz inne – w dużej części anglojęzyczne - materiały dostępne na wielu różnych portalach internetowych.

Sposób wykorzystania źródeł jest rzetelny. Nie budzą zastrzeżeń ani proporcje między cytatami a omówieniami ani między wkładem źródłowym a autorskim, choć w tym ostatnim zdarzają się niefortunne sformułowania, zapewne przejęte ze źródeł.

Analiza doboru i wykorzystania źródeł oraz efektów kwerendy pozwala stwierdzić, że Doktorantka wykazała się gruntowną wiedzą prawniczą, w szczególności w zakresie objętym tematem rozprawy.

4. Umiejętność samodzielnego prowadzenia pracy naukowej.

Wytyczanie istotnych celów badawczych, konsekwentne dążenie do ich osiągnięcia m.in. poprzez dobór właściwych metod a także jasne i logicznie poprawne formułowanie wniosków oraz należyte ich uzasadnianie - przyjmuję jako kryteria oceny umiejętności samodzielnego prowadzenia pracy naukowej.

Znaczenie społeczne i gospodarcze bezpieczeństwa w cyberprzestrzeni w okresie, który upłynął między podjęciem badań a ich ukończeniem radykalnie wzrosło, a prace legislacyjne zorientowane na dostosowanie regulacji prawnej do nowych potrzeb zintensyfikowano. Wypełnianie luk poznawczych związanych z jurydyzacją cyberbezpieczeństwa ma zatem istotne znaczenie teoretyczne ale i praktyczne, w tym dla stanowienia i realizowania prawa. Podkreślić warto, że oryginalne, szerokie ujęcie cyberbezpieczeństwa w rozprawie wymagało intuicji badawczej bowiem nie było brane pod uwagę przy tradycyjnej analizie dogmatycznej i dopiero od niedawna pojawia się w dyskursie naukowym, w którym Doktorantka może z powodzeniem uczestniczyć.

Zdobyte w trakcie przewodu doświadczenia związane z wykorzystaniem prawniczych metod badawczych: dogmatycznej a pomocniczo także historycznej i porównawczej, w rozwiązywaniu problemów interdyscyplinarnych a także wykazane w pracy umiejętności zastosowania zasad techniki prawodawczej w praktyce predestynują też Doktorantkę do aktywnego udziału w procesach stanowienia prawa.

W tekście rozprawy zauważono uchybienia językowe: z jednej strony mankamenty redakcji technicznej [str. 9,10,14,20,35,51,77,79,81,90,96,102,104,149,164,200,261,276, 352,375,381] a z drugiej nieprzywiązywanie należytej wagi do siatki pojęciowej oraz spójności i konsekwencji terminologicznej [na s. 10,12,103,106,163,361,369,371,372,380] ale ogólny poziom w tym zakresie oceniam pozytywnie. Także poziom jasności wywodów jest na obecnym etapie rozwoju naukowego zadowalający, a umiejętność precyzyjnej werbalizacji i dostosowanej do oczekiwań czytelnika selekcji wyników intelektualnych dociekań, będzie zapewne pogłębiać korzystanie ze wskazówek redaktorów i recenzentów wydawniczych.

Wagę efektów badań potwierdza wielość przekonująco uzasadnionych w rozprawie wniosków i postulatów dotyczących definiowania dziedziny regulacji oraz kształtowania strategii i polityki cyberbezpieczeństwa a także włączenie się w ten sposób w najnowszy trend badań nad skutecznością regulacji dziedzinowej.

Cała rozprawa, w szczególności konkluzje rozdziałów, należycie potwierdzają umiejętność samodzielnego prowadzenia przez Doktoranta pracy naukowej.

5. Podsumowanie

W myśl art. 13. ust. 1. ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniu i tytułach w zakresie sztuki (tekst jedn. Dz. U. z 2017 r. poz. 1789) rozprawa doktorska, przygotowywana pod opieką promotora, powinna stanowić oryginalne rozwiązanie problemu naukowego, wykazywać ogólną wiedzę teoretyczną kandydata w danej dyscyplinie naukowej oraz umiejętność samodzielnego prowadzenia pracy naukowej.

Odnosząc te wymogi do pracy doktorskiej Pani mgr Dominiki Skoczylas „Krajowy system cyberbezpieczeństwa" można stwierdzić, że przedmiotem badań uczyniono istotny problem naukowy znaczenia pojmowania bezpieczeństwa i cyberbezpieczeństwa dla skuteczności wielopoziomowej regulacji prawnej.

Przedstawione w rozprawie wyniki obejmują szczegółową analizę i krytyczną ocenę aktualnego stanu prawnego oraz oryginalne rozwiązania zdiagnozowanych problemów poprzez systemowe wytyczenie dziedziny regulacji i wskazanie potrzebnych zmian.

Podstawy źródłowe rozprawy są dobrane odpowiednio do celu badań i ponadprzeciętnie rozległe a ich rzetelna analiza, ukazując nowe - nie podnoszone wcześniej w publikacjach prawniczych - aspekty cyberbezpieczeństwa, potwierdza znaczną ogólną wiedzę teoretyczną Autorki.

O umiejętności samodzielnego prowadzenia badań naukowych świadczy skupienie się na kwestiach problematycznych, sformułowanie trafnych uwag de lege lata oraz uzasadnionych postulatów de lege ferenda, wpisujących się w nowy nurt poszukiwań skuteczności prawa.

Przedstawione w tej opinii uwagi krytyczne nie podważają przekonania o znacznej wartości naukowej pracy.

Recenzowana rozprawa magister Dominiki Skoczylas spełnia wszystkie warunki przewidziane dla prac doktorskich, zawarte w art. 13 ust. 1 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (tekst jedn. Dz.U. z 2017 r., poz. 1789) i może stanowić podstawę dopuszczenia do dalszych etapów przewodu o nadanie stopnia doktora.

Ze względu na nowatorskie ujęcie problemu regulacji prawnej cyberbezpieczeństwa praca zasługuje na wyróżnienie, o co wnioskuję.

Grażyna Szpor

Prof. dr hab. Grażyna Szpor