Kraków, dnia 20 stycznia 2021 r.

dr hab. Bogdan Fischer, prof. UP

Uniwersytet Pedagogiczny im. KEN w Krakowie

Uniwersytet Jagielloński w Krakowie

**R E C E N Z J A**

**rozprawy doktorskiej mgr Dominiki Skoczylas**

**pt. Krajowy System Cyberbezpieczeństwa**

**przygotowanej pod kierunkiem promotora**

**dr hab. Aleksandry Monarchy – Matlak, prof. US**

**oraz promotora pomocniczego**

**dr Przemysława Zdyba**

Recenzja została sporządzona z uwzględnieniem kryteriów, jakie powinna spełniać rozprawa doktorska, określonych w ustawie 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 z późn. zm.).

Na podstawie uchwały Rady Naukowej Instytutu Nauk Prawnych Uniwersytetu Szczecińskiego z dnia 20 listopada 2020 roku powołującej mnie na recenzenta w przewodzie doktorskim, wszczętym uchwałą Rady Wydziału Prawa i Administracji Uniwersytetu Szczecińskiego z dnia 29 marca 2019 roku, mam zaszczyt przedstawić niniejszą recenzję.

## I. Zagadnienia wstępne, temat, teza, metody badawcze

1. Przedmiotem rozprawy jest analiza zagadnienia cyberbepieczeństwa oraz rozwiązań opartych na uregulowaniach „Krajowego Systemu Cyberbezpieczeństwa", pozwalających wykazać potencjalne źródła zagrożeń dla prawidłowego funkcjonowania cyberprzestrzeni. Jako przyczynę zajęcia się tą problematyką Doktorantka wskazuje brak odniesień do kluczowych elementów bezpieczeństwa sieciowego, w istniejących publikacjach odnoszących się do tematu cyberbezpieczeństwa (s.16).
2. Jako zasadnicze cele rozprawy wskazano:

- analizę rozwiązań prawnych dotyczących cyberbezpieczeństwa oraz ich zasadności,
- analizę wprowadzonych przez organy administracji publicznej zmian i udoskonaleń obowiązujących przepisów, wynikających z potrzeby bezpieczeństwa publicznego i wykluczenia bądź ograniczenia zagrożeń,
- ocenę skuteczności przyjętych regulacji prawnych, zarówno w kontekście ustawy o krajowym systemie cyberbezpieczeństwa, jak i innych aktów prawnych odnoszących się do tej tematyki.

3. Jako główne zadanie badawcze Doktorantka wskazuje, charakterystykę przepisów ustawy o krajowym systemie cyberbezpieczeństwa i innych krajowych aktów prawnych istotnych w kontekście świadczenia usług drogą elektroniczną.
4. Zasadnicze problemy badawcze przedmiotowej rozprawy doktorskiej dotyczą 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

3. Podstawowa teza dysertacji: „współczesne zagrożenia bezpieczeństwa uzasadniają interdyscyplinarny charakter tego pojęcia" (s.11), jest dość oczywista. Tak sformułowana, niestety nie pomaga w precyzyjnym określeniu obszaru badawczego. W jej prawidłowym zdekodowaniu ma pomóc, dalsze sprecyzowanie, poprzez wysnucie z tej tezy przypuszczenia „bezpieczeństwo 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 i oraz głównych zadań państwa (zadań z zakresu użyteczności publicznej)." (s.12). Teza ta nie jest przez Doktorantkę traktowana jako konkretny problem badawczy (zresztą nie musi), wystarczy, że jest z nim powiązana. Dopiero połączenie tezy z zadaniami i celami pozwala w pełni określić co poddawane jest sprawdzeniu. To w nich Autorka celnie wskazuje co jest warte zweryfikowania. Dopiero spojrzenie całościowe zawarte na kilkunastu pierwszych stronach wskazuje aspekty, które uznała Autorka za istotne oraz w jaki innowacyjny sposób

będzie się przyczyniać w dysertacji do poszerzenia stanu naszej wiedzy. Łączą się one również z drugą wyodrębnioną tezą (określoną jako kolejna): „przyjmowane regulacje prawne w polskim porządku prawnym odzwierciedlają aktualne koncepcje i strategie bezpieczeństwa ustalone przez społeczność międzynarodową czy Unię Europejską". W dalszej części pracy autorka formułuje jeszcze kilka tez, które uznać jednak należy na podporządkowane podstawowym. Pomimo pewnych nieprecyzyjnych sformułowań w szczegółach, Doktorantka zbudowała w sposób wyrazisty, całościowy model badawczy na którym oparła swoją dysertację.

4. Podstawowe metody zadeklarowane (s.13) i wykorzystywane w pracy to metoda dogmatyczno-prawna, którą uzupełniają metody: prawno-porównawcza oraz historyczno-prawna. Jest to w pełni uzasadniony wybór, konsekwentnie realizowany w pracy.

5. Doktorantka prawidłowo zidentyfikowała i poddała analizie regulacje prawne mające zasadnicze znaczenie dla przyjętego obszaru badawczego. W zakresie ustaw polskich: ustawę o krajowym systemie cyberbezpieczeństwa, ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę o świadczeniu usług drogą elektroniczną, ustawę o usługach zaufania oraz identyfikacji elektronicznej, ustawę o dostępie do informacji publicznej, ustawę o ochronie danych osobowych. W zakresie aktów prawa unijnego szczególną uwagę poświęciła: RODO, dyrektywie NIS, rozporządzeniu eIDAS oraz aktowi o cyberbezpieczeństwie. Doktorantka dokonała również prawidłowego doboru orzeczeń sądowych, w tym sądów administracyjnych, Trybunału Konstytucyjnego, instytucji unijnych. Aktualność ustaleń potwierdziła informacjami i wykazami pochodzącymi ze stron internetowych właściwych instytucji, ministerstw, organów krajowych i międzynarodowych. W tak dynamicznym obszarze te ostatnie działania były niezbędne.

## II. Układ rozprawy, bibliografia, przypisy

1. Ta obszerna rozprawa (453 strony) ma spójną logiczną strukturę. Składa się z pięciu rozdziałów podzielonych na podrozdziały i punkty oraz wstępu i zakończenia.

2. Systematyka rozprawy jest dostosowana do omawianego zagadnienia. Struktura pracy jest przejrzysta, odzwierciedla zakreślone we wstępie cele badawcze. Wstęp w sposób zasadniczo uporządkowany ( z małym zastrzeżeniem wskazanym przy tezie) wprowadza czytelnika w tematykę rozprawy, przedstawia intencje i motywacje badawcze. Widoczna

we wstępie jest zapobiegliwość o odbiór dalszych części, oraz przekonanie recenzentów i innych czytelników, że to dzieło wartościowe. Rozdział I zatytułowany: „Bezpieczeństwo jako element prawidłowego funkcjonowania państwa" zawiera omówienie zagadnień podstawowych dotyczących znaczenia bezpieczeństwa w demokratycznym państwie prawnym. Autorka dużą uwagę zwraca na kwestie definicyjne i klasyfikacyjne co ułatwia Jej wyjaśnianie i porządkowanie badanej materii, oraz przygotowanie instrumentarium do dalszych wywodów. W rozdziale tym dokonała interesującego przeglądu koncepcji naukowych, starając się jednak przedstawiać je neutralnie, rezygnując z podejścia krytycznego. Autorka odnosząc się w tej części do historii między innymi zimnej wojny między USA i ZSRR, czy kreowania przez Papieża Jana Pawła II bezpieczeństwa państwa jako wyznacznika bezpieczeństwa narodu, czyni to w sposób wyważony. Nawiązanie do funkcjonujących sojuszy polityczno-wojskowych, będących korzeniami współczesnego bezpieczeństwa, pozwala odbiorcy uchwycić kontekst, który jest logiczną zapowiedzią dalszych części. W rozdziale II „Założenia Krajowego Systemu Cyberbezpieczeństwa", Autorka dokonuje podstawowych ustaleń dla pracy, opartych na założeniu że obecnie cyberprzestrzeń jest podstawowym miejscem, gdzie potencjał zagrożeń bezpieczeństwa jest największy. Celne diagnozy stawiane są w odniesieniu do sektora usług publicznych, czy w ogóle funkcjonowania administracji publicznej. Zwraca uwagę, iż aktualnie sprawność administracji warunkują nowe technologie, wraz z towarzyszącymi specyficznymi zagrożeniami, które Doktorantka po wyodrębnieniu poddaje analizie w dalszej części pracy. Konieczność stworzenia i zastosowania zintegrowanego systemu zarządzania bezpieczeństwem teleinformatycznym, przygotowującym na zagrożenia ataków na sieci i systemy teleinformatyczne nie jest poddawana w wątpliwość. Zwłaszcza gdy jego brak powodowałby poważne zaburzenia w funkcjonowaniu elementów tworzących infrastrukturę krytyczną. Autorka wyróżnia znaczenie poszczególnych wyzwań w aspekcie ochrony bezpieczeństwa, wśród których jako główne uznaje „kontrolę w zakresie organizacji, użycia narzędzi teleinformatycznych zgodnie z przeznaczeniem oraz zapewnienie ciągłości działania" (s.82). Przy szeroko opisanych wyzwaniach do podjęcia, sposobach redukowania ryzyk oraz przeciwdziałania zagrożeniom, zbyt mało miejsca zostało poświęcone sposobom wykorzystywania szans czyli okoliczności sprzyjających. Za poszukiwanie szans prawnych, można uznać diagnozę na bazie uregulowań poziomu unijnego, regionalnego czy międzynarodowego. Doktorantka zaczynając od oceny zadań bezpieczeństwa realizowanych na arenie międzynarodowej,

dochodzi do interesujących postulatów de lege ferenda w odniesieniu do krajowego systemu cyberbezpieczeństwa i opisującej go ustawy. Kontynuacją krytycznej analizy nielicznych rozwiązań ustawy o krajowym systemie bezpieczeństwa, jest wskazanie potrzeby zmian w zasadach wprowadzania strategii cyberbezpieczeństwa w rozdziale III pt.: „Cyberbezpieczeństwo i bezpieczeństwo sieciowe". Doktorantka postawiła w nim nacisk na rozgraniczenie dwóch aspektów: cyberbezpieczeństwa powszechnego i indywidualnego a także na rodzaje zagrożeń bezpieczeństwa sieciowego. Analizy były prowadzone pod kątem określenia zasad i zadań organów administracji publicznej podejmowanych w celu wykrycia i zneutralizowania zagrożenia (np. cyberterroryzmu). Ponownie pojawia się konstatacja, że nie wystarczą rozwiązania organizacyjne i techniczne, gdyż „subiektywne czy obiektywne poczucie bezpieczeństwa zależy przede wszystkim od wprowadzonych rozwiązań prawnych" (s.156). W rozdziale IV pt.: „Bezpieczeństwo sektorowe", autorka przeprowadziła badanie obowiązków organów, instytucji i podmiotów mających za cel nieprzerwane i wydajne świadczenie usług o kluczowym znaczeniu dla społeczeństwa w tym cyfrowe, energetyczne, finansowe, transportowe i zdrowotne. Rozdział ten w wyniku poczynionych ustaleń doprowadził podobnie jak poprzednie rozdziały do sformułowania wartościowych wniosków de lege lata i de lege ferenda. Kolejność poszczególnych rozdziałów od I do IV jest przemyślana, a ustalenia poczynione w jednym rozdziale są konsekwencją poprzedniego, tworząc spójną całość. Rozdział V, pt.: „Bezpieczeństwo elektroniczne w administracji", stanowi analizę najważniejszych koncepcji i zasad prawa administracyjnego, oraz ich wpływu na realizację zadań publicznych, zarówno w wymiarze tradycyjnym jak i elektronicznym. Wydaje się że ten rozdział o charakterze bardziej ogólnym powinien, w dużej części znaleźć się na początku pracy, w szczególności w zakresie wyjaśnienia pojęć podstawowych dla prawa administracyjnego jak np. władztwo administracyjne.

3. W pracy wykorzystano bardzo obszerną literaturę zarówno krajową jak i zagraniczną obejmującą 396 pozycji. Literatura jest zróżnicowana i większość pochodzi z ostatnich lat, co z jednej strony jest uzasadnione nowością tematyki z drugiej odzwierciedla prawidłowe podejście Doktorantki do dynamizmu zmian. Powołała się ponadto na 48 aktów prawa krajowego, 26 aktów prawa międzynarodowego i unijnego. Jeśli chodzi o wyroki: 1 TSUE, 10 Trybunału Konstytucyjnego, 7 Naczelnego Sądu Administracyjnego, 4 Sądu Najwyższego, 5 Wojewódzkiego Sądu Administracyjnego. Inne źródła, wydzielone z uwzględnieniem ich internetowego miejsca udostępnienia zawierają 99 pozycji.

Doktorantka z niewiadomych przyczyn wydzieliła grupę 6 dodatkowych dokumentów w tym załączników, które mogły zostać zakwalifikowane do powyższych. To małe zastrzeżenie nie ma wpływu na całościową ocenę doboru źródeł, który należy ocenić jako prawidłowy.

4. Wnioski de lege lata i postulaty de lege ferenda przedstawione w poszczególnych rozdziałach pracy, pozwoliły zgodnie z założeniem Autorki na sformułowanie wniosków podsumowujących w zakończeniu dysertacji. Zawarto tam również odpowiedzi na postawione we wstępie pytania oraz zwięzłe konkluzje w odniesieniu do zagadnień kluczowych.

**III. Ocena formalna**

1. Praca została opracowana bardzo starannie, z dbałością o stronę językową oraz solidną stroną edytorską. Drobne literówki są rzadkością.
2. Materia pracy została rozłożona równomiernie, a następujące po sobie zagadnienia są systematycznie rozwijane. Pomimo technicznego charakteru istoty badanego zagadnienia, Autorka zadbała o bieżące wyjaśnianie potencjalnych wątpliwości.
3. Na każdym etapie pracy widać, że Doktorantka przywiązuje dużą wagę do szczegółów i jasności wywodu. Ta precyzja doprowadza niekiedy do sytuacji w której ma miejsce nadmierne użycie omawianego pojęcia. Przykładowo „rejestr" używane jest 27 razy na zaledwie trzech stronach 328-330.
1. Brakuje zwięzłych wprowadzeń do rozdziałów, które mogłyby dodatkowo wpłynąć pozytywnie na jasność wywodu. Jednak treść rozdziałów, stanowi spójną całość, sposób formułowania myśli nie budzi wątpliwości, zapewniając pozytywny odbiór i pozwalając stosunkowo szybko wejść w miejscami skomplikowaną technicznie tematykę.
2. Autorka jest rzetelna w przytaczaniu materiału zastanego, a przypisy stosowane są prawidłowo i konsekwentnie w całej pracy. Literatura wykorzystana w pracy pochodzi z wielu dyscyplin począwszy od podstawowej – nauk prawnych, poprzez informatykę techniczną i telekomunikację, nauki o zarządzaniu i jakości, nauki o bezpieczeństwie czy nauki o polityce i administracji. Przyjęte podejście jest prawidłowe gdyż zadania i problemy wynikające z podjętej tematyki są coraz bardziej złożone, co powoduje przekraczanie kompetencji jednej dyscypliny. Przy czym bezwzględnie dominujący jest dyskurs prawny.

3. Przyjmując założenie że praca doktorska jest zwieńczeniem pewnego etapu pracy naukowej i umiejętności warsztatowych, czytając tą dopracowaną i przemyślaną dysertację Doktorantka wyszła z tej próby zwycięsko, co również dobrze rokuje na przyszłość,

## IV. Uwagi merytoryczne

1. Eksplorację teoretyczną tematyki należy ocenić wysoko, a na szczególne uznanie zasługuje umiejętność wykorzystywania aktualnej literatury dot. cyberbezpieczeństwa w powiązaniu z tradycyjnym ujęciem prawa administracyjnego. Doktorantka bardzo sumiennie i odpowiedzialnie przedstawiła opis obowiązującego stanu prawnego, stanowiska doktryny oraz wypowiedzi judykatury.
2. W pracy widoczna jest dyscyplina w realizowaniu przyjętych założeń oraz utrzymania systematycznego podejścia do badanych zagadnień.
3. Należy podkreślić znaczenie społeczne podejmowanych problemów, jak np. pola walki w cyberprzestrzeni (np. s. 182), wojen hybrydowych (s.92), działań represyjnych (np. s. 264), problemu przemocy (np. s. 69, 123, 189, 264), dezinformacji (np. s. 174, 191, 192) czynników wpływających na suwerenność państwa, niepodległość, integralność terytorium (np. s.26, 58, 61, 70). Cyberbezpieczeństwo włączone jest w realne problemy współczesnych społeczeństw i świata, stąd przedstawienie ujęcia kompleksowego, systemowego przy pozostawieniu otwartej perspektywy jest zasadne.
4. Autorka w dysertacji wykazuje w jakim stopniu wzrost możliwości technicznych wpływa na konieczność ciągłego udoskonalania rozwiązań różnej natury (w tym prawnej) zapewniających wewnętrzne i zewnętrzne bezpieczeństwo w cyberprzestrzeni.
5. Doktorantka nie mogła się zdecydować gdzie postawić granice w badanej tematyce, co spowodowało, że w pracy zostały poddane szczegółowej analizie także te zagadnienia, których związek z cyberbezpieczeństwem jest stosunkowo odległy.
6. Autorka trzymała się przyjętych we wstępie założeń, chociaż nie uniknęła kwestii pobocznych. Co prawda wpłynęło to w jakiś sposób zdaniem recenzenta na objętość dysertacji, nie można tego ocenić jako niezasadne, lecz nie zawsze w pełni potrzebne.
7. Przy badaniu mechanizmów gospodarki cyfrowej, gdzie wyznacznikiem są technologie informacyjno-komunikacyjne, Autorka sporo uwagi poświęciła obszernemu omówieniu zagadnień podstawowych dla badanej tematyki jak świadczenie usług drogą elektroniczną, informatyzacja, cyfryzacja, e-administracja, czy jawność i dostęp do informacji publicznej.

8. Doktorantka realizując przyjęte ambitne założenia starała się rozstrzygnąć możliwie jak najwięcej kontrowersji, wykazując przy tym pośrednio lub bezpośrednio kilkadziesiąt ważnych kierunków działań. Za istotne spośród nie wprost wyrażonych uznaję: badania wydzielonego problemowo zagadnienia cyberbezpieczeństwa dla przeciwdziałania cyberprzestępczości; rozplanowania przygotowań przedsiębiorców i infrastruktury krytycznej na cyberataki; zmianę nierównowagi między obecnym rozwojem technicznym a koordynacją krajową i międzynarodową. Kolejny kierunek to weryfikacja kształtowania wciąż nowych rozwiązań organizacyjnych i technicznych zwiększających cyberodporność, które powstają przy wciąż niedoskonałym poziomie dialogu między zainteresowanymi podmiotami publicznymi i prywatnymi oraz przy nie nadążaniu prawodawcy, w przygotowaniach odpowiednich ram prawnych. Doprowadzenie badań do momentu pozwalającego odpowiedzieć na pytanie jaki powinien być najbardziej odpowiedni poziom regulacji cyberbezpieczeństwa: lokalny, krajowy, unijny czy międzynarodowy.
9. Opierając się na założeniu wielopłaszczyznowości pojęcia bezpieczeństwa technologicznego a ściślej cyberbezpieczeństwa, przeprowadza delimitację poszczególnych płaszczyzn, oraz ustala ich wzajemne zależności. Celnie rozdziela atrybuty i strategie, mające znaczenie dla organów publicznych, użytkowników końcowych czy dla usługodawców.
10. Chociaż podtrzymuję pozytywny odbiór zakończenia na który wskazałem w części I recenzji, jest ono słabsze aniżeli można się było spodziewać po całej pracy. Jako podsumowanie dysertacji, pozostawia pewien niedosyt, gdyż z jednej strony pominięto wiele ważnych efektów analiz i dokonanych ustaleń, z drugiej zawarto w nim szereg nie odkrywczych sformułowań, mających być niejako wynikiem przeprowadzonych badań. Przykładowo odnośnie dedykowanej temu zagadnieniu ustawie: „Dokonana w niniejszej dysertacji analiza, pozwala na przyjęcie stwierdzenia, że aktualnie najbardziej konkretne rozwiązania prawne w kwestii wzmocnienia bezpieczeństwa systemów teleinformatycznych, usług kluczowych i usług cyfrowych zawiera ustawa o krajowym systemie cyberbezpieczeństwa"( s. 369) czy „Należy zwrócić uwagę, że materia bezpieczeństwa elektronicznego (cyberbezpieczeństwa) nieobca jest administracji publicznej" (s.370). Odnosi się wrażenie że Doktorantka nie mogła się zdecydować co umieścić w zakończeniu i nie wszystkie decyzje były przemyślane.
11. Doktorantka zrealizowała wiele zadań, których znaczenie sama niepotrzebnie zmarginalizowała, a powinny zostać sformułowane, we wstępie jako podstawowe np.

usystematyzowanie zależności pomiędzy poszczególnymi elementami cyberbezpieczeństwa. Podkreślenie znaczenia wypracowanych w ich wykonaniu rozwiązań ma duże znaczenie nie tylko z teoretycznego i naukowego punktu widzenia, ale także praktycznego.

12. Doktorantka trafnie i odważnie recenzuje obowiązujące regulacje prawne formułuje celne wnioski oraz zgłasza liczne postulaty.
13. Pewne zastrzeżenia można mieć co do ograniczenia uwag krytycznych dotyczących dyrektywy NIS, której zarzucić można sporo słabości, skutkujących wytężonymi pracami nad jej zmianą (tzw. NIS2). Brzmienie NIS spowodowało m.in. znaczne różnice w implementacji w poszczególnych krajach członkowskich i rozważano czy nie będzie konieczne wprowadzenie rozporządzenia (z którego ostatecznie zrezygnowano). Różnice wynikały m. in. z braku jednolitości podejścia w poszczególnych krajach dot. opracowania systemu identyfikacji operatorów usług kluczowych (pozytywnie ocenionego przez Autorkę np. na s.380) i w konsekwencji np. dużej rozbieżności liczby tych podmiotów w poszczególnych krajach. Projektowany NIS 2 ma określać dokładnie krąg podmiotów, podlegających jej regulacjom. Autorka nie zaakcentowała uwag, pomimo, że wskazywały na to już wczesne raporty z końca 2019 roku: KE oceniającej spójność podejść przyjętych przez państwa członkowskie w procesie identyfikacji operatorów usług kluczowych czy ENISA na temat zarządzania incydentami w państwach członkowskich. Później zastrzeżenia ewaluowały.
14. Nie wybrzmiała adekwatnie do potrzeb, istota zwiększenia wymiany informacji w zakresie cyberbezpieczeństwa i inicjatyw w tym zakresie, a także ujęcia bezpieczeństwa informacyjnego państwa, jako transsektorowego, transdziedzinowego i transpodmiotowego obszaru bezpieczeństwa.
15. Wysoko oceniam umiejętność Doktorantki jaką jest zdolność zestawiania problemów badawczych w oparciu o celnie identyfikowane problemy zarówno praktyczne jak i teoretyczne.
16. Pomimo pewnych uwag, których jak na tak obszerną pracę jest niewiele, wysoko oceniam recenzowaną pracę. Jest to bardzo interesująca z naukowego jak i praktycznego punktu widzenia. dojrzała i świetnie zrealizowana praca. Doktorantka w oparciu o dobrze dobrane pytania badawcze wyjaśniła i powiązania najważniejsze zagadnienia z zakreślonego obszaru, stając się jednocześnie źródłem twórczych inspiracji

## V. Podsumowanie

Rozprawa stanowi oryginalne rozwiązanie problemu naukowego oraz wykazuje ogólną wiedzę teoretyczną Doktorantki w dyscyplinie naukowej - nauki prawne. Doktorantka wykazała się umiejętnością spójnego formułowania myśli oraz dużą wiedzą, którą potrafiła wykorzystać dla realizacji przyjętych założeń. Na aprobatę zasługuje zarówno wybór przedmiotu badań, jak i jasność przeprowadzonego, dobrze udokumentowanego wywodu. Konstrukcja pracy jest prawidłowa, oparta na dobrze dobranej literaturze krajowej i zagranicznej. Dysertacja ukazuje kompetencje merytoryczne i duży potencjał badawczy oraz w pełni potwierdza umiejętność samodzielnego prowadzenia pracy naukowej.

Zgodnie z ustawą z dnia 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (tekst jedn.: Dz. U. z 2017 r. poz. 1789 z późn. zm.) oraz rozporządzeniem Ministra Nauki i Szkolnictwa Wyższego z dnia 26 września 2016 roku w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodzie doktorskim, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora (Dz.U. z 2016 r. poz. 1586), **przedłożoną rozprawę doktorską mgr Dominiki Skoczylas pt. Krajowy System Cyberbezpieczeństwa, ocenić należy zdecydowanie pozytywnie a Doktorantkę dopuścić do dalszych etapów postępowania doktorskiego.**