Prof. UKSW dr hab. Elżbieta Karska

Katedra Ochrony Praw Człowieka
i Prawa Międzynarodowego Humanitarnego
Wydział Prawa i Administracji
Uniwersytet Kardynała Stefana Wyszyńskiego
w Warszawie

Warszawa, dnia 15 listopada 2019 r.

Recenzja rozprawy doktorskiej mgra Tomasza Welanyka pt. *Istnienie i granice suwerenności w cyberprzestrzeni. Analiza prawna*, napisanej pod opieką naukową prof. UEK dra hab. Pawła Czubika (promotora) oraz dra Pawła Filipka (promotora pomocniczego)

W związku z powołaniem w dniu 16 września 2019 r. przez Radę Naukową Instytutu Prawa Międzynarodowego Wydziału Prawa i Administracji Uniwersytetu Warszawskiego na recenzentkę rozprawy doktorskiej mgra Tomasza Welanyka pt. *Istnienie i granice suwerenności w cyberprzestrzeni. Analiza prawna* (dalej: „rozprawa doktorska"), napisanej pod opieką naukową prof. UEK dra hab. Pawła Czubika (promotora) oraz dra Pawła Filipka (promotora pomocniczego), przedstawiam niniejszym jej ocenę:

1. Wybór tematu rozprawy doktorskiej

Rozwój technologii, zwłaszcza w kilku ostatnich dziesięcioleciach, wiąże się ze znacznym rozwojem technologicznym ludzkości. Tempo tego rozwoju nigdy nie było tak szybkie, jak w ciągu ostatnich kilkudziesięciu lat. Ten niewątpliwy sukces wiąże się z występowaniem zjawisk i zagrożeń, które nigdy wcześniej nie miały miejsca. Taki stan rzeczy staje się wymagający dla nauk prawnych, które bardzo często nie nadążają, czy nawet nie są w stanie nadążać za nowymi wyzwaniami współczesnego świata. Jednym z takich wyzwań jest problematyka dotycząca cyfrowych zagrożeń, występujących w cyberprzestrzeni.

Cyberprzestrzeń i procesy w niej zachodzące mają znaczenie i bezpośredni wpływ na większość aspektów działania jednostki. Mają one także wpływ na funkcjonowanie podmiotów prawa międzynarodowego. Zorganizowane ataki cyberterrorystyczne są w stanie uniemożliwić prawidłowe działanie organów państwa, poważnie zagrozić jego bezpieczeństwu, czy – w skrajnych przypadkach – istnieniu. Dlatego też trudno byłoby nie podejmować badań

dotyczących rozmaitych zagrożeń występujących w cyberprzestrzeni w kontekście prawa międzynarodowego publicznego.

Jako interesujący jawi się problem istnienia i gwarancji suwerenności w cyberprzestrzeni. Jest to problematyczne i wielowątkowe zagadnienie, ponieważ samo funkcjonowanie państwa w cyberprzestrzeni wiąże się z licznymi ograniczeniami (s. 191). Suwerenne kompetencje państwa mogą natomiast być realizowane w regulacjach krajowych. W tym ujęciu, znaczenie będzie miała jurysdykcja konkretnych podmiotów, która będzie odgrywała rolę w kontekście lokalizacji serwerów czy numerów IP, zwłaszcza w kontekście zastosowania regulacji krajowych. Jak widać, jest to problematyka wielowątkowa, której zbadanie jest niezbędne w kontekście wyzwań współczesnego prawa międzynarodowego publicznego.

Biorąc pod uwagę, że zarówno w literaturze polskiej, jak i zagranicznej zdecydowanie brakuje opracowania poświęconego problematyce istnienia i granic suwerenności w cyberprzestrzeni, należy zaznaczyć, że rozprawa doktorska mgra Tomasza Welanyka stanowi kompleksową analizę tego obszaru, wypełniając tym samym lukę w doktrynie nauki prawa międzynarodowego publicznego. Wybór przez Doktoranta tematu rozprawy doktorskiej jest interesujący, albowiem podejmuje zagadnienia ważne i praktyczne dla naukowców, specjalistów od bezpieczeństwa w cyberprzestrzeni czy informatyków. Jest to istotna tematyka, która zasługuje na poważną analizę naukową. Pozytywnie należy ocenić, że Doktorant dostrzegł taką potrzebę.

2. Ocena merytoryczna rozprawy doktorskiej

2.1 Konstrukcja rozprawy

Rozprawa doktorska mgra Tomasza Welanyka składa się ze wstępu, pięciu rozdziałów i wniosków. W rozdziale pierwszym pt. „Definicje pojęć" Doktorant precyzyjnie określa zakres badanego problemu. Ponadto, definiuje kluczowe dla dalszej części badań pojęcia. Dotyczy to takich terminów jak cyberprzestrzeń, jurysdykcja terytorialna w cyberprzestrzeni, jurysdykcja funkcjonalna czy jurysdykcja nad fizyczną częścią cyberprzestrzeni. W rozdziale drugim pt. „Prawo cyberprzestrzeni" Doktorant omawia funkcjonowanie podstawowych norm prawnych oraz zastosowanie fundamentalnych zasad prawa międzynarodowego do sfery cyberprzestrzeni. W tej części badań, Autor dokonuje rekonstrukcji zasad wynikających z orzecznictwa oraz odwołuje się także do klauzuli Martensa. Podjęto także analizę *lex informatica* oraz jego źródeł a także mechanizmów tworzenia norm w jego obrębie.

Rozdział trzeci jest poświęcony cyberprzestrzennym zagrożeniom dla suwerenności. Tę część badań rozpoczyna analiza pojęcia suwerenności, jej koncepcji we współczesnym prawie międzynarodowym publicznym oraz jej wykonywania w cyberprzestrzeni. Zbadano również przypadki cyberprzestrzennych naruszeń suwerenności nie stanowiących cyberataku a także naruszenia suwerenności poniżej poziomu ataku. Bardzo wartościowym elementem badań Doktoranta w tej części pracy jest analiza remediów przeciwko operacjom nie stanowiącym użycia siły. W rozdziale czwartym pt. „Prawo konfliktu cyberprzestrzennego" Autor analizuje szeroko pojętą problematykę konfliktu odbywającego się w cyberprzestrzeni pod kątem prawnym. Aby tego dokonać, Doktorant dokonuje analizy *Ius ad bellum*, a więc prawa do konfliktu w cyberprzestrzeni, *Ius in bello*, w kontekście regulacji dotyczących prowadzenia walki w cyberprzestrzeni oraz ograniczenia możliwości prowadzenia działań zbrojnych w cyberprzestrzeni. W rozdziale piątym pt. „Cyberlawfare" Doktorant dokonał połączenia terminów „cyber" i „lawfare", celem dokładniejszego oddania treści badanego problemu. Autor koncentruje się na zastosowaniu cyberlawfare w operacjach cyberprzestrzennych. Zwrócono także uwagę na problematykę dotyczącą aktorów niepaństwowych w tym zakresie oraz na terytoria sporne i mikropaństwa.

Powyższą konstrukcję rozprawy doktorskiej należy uznać za prawidłową. Doktorant konsekwentnie odzwierciedlił w treści rozprawy jej tytuł – „Istnienie i granice suwerenności w cyberprzestrzeni. Analiza prawna,". Każdemu z elementów składowych tytułu rozprawy doktorskiej poświecono osobny rozdział, co sprawia, iż wywody Autora zostały przedstawione w sposób spójny, logiczny i przemyślany.

Prosta, a zarazem wypełniona treścią, struktura rozprawy doktorskiej odzwierciedla umiejętności Doktoranta w dokonaniu precyzyjnej i właściwej analizy źródeł. Autor bardzo dobrze wykorzystuje materiały źródłowe, akty prawa krajowego oraz źródła prawa międzynarodowego publicznego oraz bardzo bogatą literaturę przedmiotu. Ten materiał badawczy został przez Doktoranta dobrze wykorzystany.

2.2 Merytoryczna ocena problemu badawczego

Wartość merytoryczną rozprawy doktorskiej mgra Tomasza Welanyka należy ocenić wysoko. Podjęte przez Doktoranta rozważania na temat istnienia i granic suwerenności w cyberprzestrzeni nie ograniczają się wyłącznie do aspektów teoretycznych podjętej problematyki. Autor wykracza poza te obszary, starając się dostrzec także praktyczne aspekty i konsekwencje wykonywania suwerenności państw w cyberprzestrzeni oraz potencjalne skutki

rozstrzygnięć, zarówno w sferze prawa krajowego, jak też prawa międzynarodowego publicznego. Bardzo wartościowe są rozważania Autora z w rozdziale IV dysertacji, poświęconym prawu konfliktu cyberprzestrzennego. Doktorant odwołuje się w nim do podstaw prawa konfliktów zbrojnych i odnosi je do realiów konfliktów w cyberprzestrzeni. Jest to z pewnością wartościowa analiza, która może stanowić ważny punkt odniesienia do dalszych badań w tym obszarze. Ten element stanowi próbę szerszego spojrzenia na podejmowaną w badaniach problematykę. Podjęcie próby takiej analizy jest niewątpliwą zaletą pracy.

Podstawowym problemem badawczym, jak wskazuje sam Autor, jest kwestia istnienia suwerenności państwowej w cyberprzestrzeni, a także możliwości wykonywania w niej jurysdykcji państwowej, która stanowi tej suwerenności odbicie i konieczny warunek istnienia (s. 1).

Tak sformułowany problem badawczy wymaga zbadania dwóch, kluczowych kwestii. Pierwsza z nich dotyczy analizy, czym w istocie jest cyberprzestrzeń, zarówno z punktu widzenia prawnego, jak i faktycznego. Drugą jest rozważenie sposobu normowania cyberprzestrzeni, a także analiza tworzącego się dopiero systemu *lex informatica*, który łączy normy prawa stanowionego, zwyczajowego i elementy technicznej konstrukcji cyberprzestrzeni (s. 1-2). Autor zwraca uwagę, że w tym kontekście pojęcie suwerenności należy traktować szerzej, zaś suwerenność w cyberprzestrzeni będzie funkcją prawa międzynarodowego i nowych, dopiero powstających norm prawa cyberprzestrzeni. Autor stawia także pytanie o istnienie suwerenności *stricte* cyberprzestrzennej (s. 3).

Zdaniem samego Doktoranta, rozprawa jest w pierwszym rzędzie odpowiedzią na pytanie, czy wraz z rozwojem prawa cyberprzestrzeni zachowanie jurysdykcji (a co za tym idzie suwerenności) przez tradycyjnie pojmowane państwa jest możliwe i jakimi środkami państwa mogą tę suwerenność zachować (s. 8).

Autor przeprowadził swoje badania w oparciu o odpowiednio dobrane metody, techniki i narzędzia badawcze. W pracy wykorzystano metody analizy źródeł prawa, analiza praktyki międzynarodowej w zakresie cyberprzestrzeni, analizę orzecznictwa, badanie literatury przedmiotu i *case studies*.

Zdaniem Autora, podstawową metodą badawczą przyjętą w pracy jest analiza praktyki międzynarodowej w zakresie cyberprzestrzeni (s. 6). Doktorant uzasadnia, że ze względu na specyfikę opartego o *lex informatica* systemu prawa cyberprzestrzeni, ma ona podstawowe

znaczenie dla określenia sposobu jej normowania. Analiza *opinio iuris* jest kluczowa, ponieważ nie istnieją znaczące traktaty czy kodyfikacje dotyczące bezpośrednio prawa cyberprzestrzeni (s. 11-12). Autor podkreśla, że metodologia rozprawy musi obejmować także rozważania i analizę literatury przedmiotu dotyczącej stanu faktycznego cyberprzestrzeni (s. 12). Celem analizy przypadków jest uzupełnienie rozważań dotyczących praktyki międzynarodowej, także w kontekście reakcji na naruszenia suwerenności w cyberprzestrzeni (s. 13).

Merytoryczną analizę Autor rozpoczyna w rozdziale I od zbadania pojęć kluczowych dla dalszej części rozważań. Rozdział ten, zatytułowany „Definicje pojęć", ma więc na celu stworzenie definicji niezbędnych dla określenia zakresu badań. Najistotniejsze dla Doktoranta jest z całą pewnością wyjaśnienie terminu „cyberprzestrzeń", które jest też fundamentalne dla dalszej części badań. Autor odwołuje się w tym zakresie do źródeł prawa krajowego oraz do definicji wypracowanych przez doktrynę prawa międzynarodowego. Oprócz pojęcia cyberprzestrzeni, analizie poddano także zagadnienie jurysdykcji w prawie międzynarodowym publicznym. To badanie nie ogranicza się jednak do sfery prawa międzynarodowego, lecz stara się także uwzględnić pojęcie jurysdykcji w cyberprzestrzeni. Autor podejmuje także analizę wykonywania jurysdykcji w cyberprzestrzeni oraz jurysdykcji nad fizyczną jej częścią.

W rozdziale drugim Doktorant dokonuje badań prawa cyberprzestrzeni. Tak naprawdę ten system prawny znajduje się *in statu nascendi*. Podstawę do rozważań w tej części pracy stanowią zasady prawa międzynarodowego publicznego, wraz z próbą ich odniesienia i zastosowania do cyberprzestrzeni. I tak, Autor odwołuje się do testów przypisania, działań naruszających suwerenność oraz do wniosków wynikających z orzecznictwa międzynarodowego, zwłaszcza w kontekście spraw Lotus i Rainbow Warrior. Te reguły Autor uzupełnia klauzulą Martensa, której zastosowanie odnosi do sfery cyberprzestrzeni. W dalszej części badań, Doktorant koncentruje się na *lex informatica*, które kreuje w analogii do *lex mercatoria*. Autor bada źródła i normy *lex informatica,* a także sposób kreowania norm w tym zakresie. Ze względu na szczególną specyfikę i dynamikę rozwoju badanej problematyki, istotną rolę odgrywa w niej także normowanie faktyczne. Dlatego też uzasadnione wydaje się zbadanie wzajemnych relacji normowania faktycznego i prawa stanowionego. Istotna jest także analiza zwyczaju międzynarodowego w sferze *lex informatica*.

Rozdział trzeci rozprawy został poświęcony cyberprzestrzennym zagrożeniom dla suwerenności. Zdaniem Autora stanowi on próbę przeanalizowania możliwości istnienia suwerenności państwowej w informatycznej części cyberprzestrzeni; jest więc próbą udzielenia odpowiedzi na pytanie, czy możliwa jest swoista „terytorializacja" cyberprzestrzeni (s. 4-5). Rzeczywiście pierwsza część badań w tym rozdziale koncentruje się na pojęciu suwerenności. Doktorant analizuje koncepcje suwerenności we współczesnym prawie międzynarodowym, po czym stara się wnioski odnieść do problematyki suwerenności w cyberprzestrzeni. Zwraca także uwagę na jurysdykcję zwyczajną i nadzwyczajną w kontekście wykonywania suwerenności w cyberprzestrzeni. Autor słusznie dostrzega problem naruszeń suwerenności, które nie stanowią ataku. Naturalnie fakt, że dane działanie nie stanowi ataku, nie oznacza, że nie powoduje ono naruszenia suwerenności. Dalsza część omawianego rozdziału bada właśnie cyberprzestrzenne naruszenia suwerenności, które nie stanowią ataku oraz naruszenia suwerenności będące poniżej poziomu konfliktu. Warto zwrócić uwagę, że w tej części badań podjęto także problematykę środków, które mogą być zastosowane przeciwko operacjom, które nie stanowią użycia siły. Autor zwraca w tym kontekście uwagę na regulacje przyjęte w systemie prawnym Unii Europejskiej (*Cybersecurity Act*), czy na strukturę ochrony pasywnej w systemie prawnym USA.

Rozdział czwarty uzupełnia dotychczasowe rozważania o analizę prawa konfliktu cyberprzestrzennego. Autor zwraca w nim uwagę zarówno na sam konflikt cyberprzestrzenny, jak też inne naruszenia suwerenności, których skutki przekraczają próg użycia siły w rozumieniu praktyki ONZ. Autor odwołuje się do instytucji właściwych dla międzynarodowego prawa humanitarnego i stara się je zastosować do warunków konfliktu cyberprzestrzennego. I tak, Doktorant zwraca uwagę na konstrukcję *Ius ad bellum* w kontekście konfliktu prowadzonego w cyberprzestrzeni oraz *Ius in bello*, a więc – w tej konfiguracji – prawo regulujące prowadzenie niekinetycznej walki cyberprzestrzennej. W tej części Autor odwołuje się także do Karty Narodów Zjednoczonych w kontekście analizy legalności użycia siły. Następnie odnosi swe rozważania do problematyki legalności użycia siły w cyberprzestrzeni. W tej części badań podjęto także analizę cyberataków wraz z próbą ich charakterystyki oraz omówieniem doktryn dotyczących cyberataków. Autor dokonuje także analizy testu Schmitta, który ma na calu dokonanie oceny, kiedy dana cyberoperacja przekracza próg użycia siły, naruszając tym samym art. 2 (4) KNZ i umożliwiając działania obejmujące samoobronę (s. 265). W kontekście omawianego testu, analizie poddano kryteria dolegliwości, legalności, natychmiastowego skutku, bezpośredniości, inwazyjności, mierzalności

i odpowiedzialności. Zbadano także prawo do samoobrony w kontekście konfliktu w cyberprzestrzeni oraz mechanizmy ograniczenia prowadzenia konfliktu w cyberprzestrzeni. Jak już stwierdziłam wcześniej, ta część pracy jest bardzo wartościowa. Jest ona także poparta sporą ilością badań i niewątpliwym przygotowaniem, jakim wykazał się Autor.

Ostatni, piąty rozdział dysertacji podejmuje problematykę „cyberlawfare". Jest to termin stanowiący połączenia pojęć „lawfare" i „cyber". Zdaniem Autora, ma on odzwierciedlać zastosowanie „lawfare" do cyberprzestrzeni (s. 5). Pojęcie „lawfare" powstało z połączenia słów „law" i „warfare" i w tej formie pojawia się w doktrynie prawa międzynarodowego publicznego. Autor wskazuje, że termin ten wiąże się ze stosowaniem prawa międzynarodowego jako narzędzia prowadzenia konfliktu oraz doprowadzenie do oceniania sytuacji militarnej konfliktu przez pryzmat prawa międzynarodowego (s. 298). Dodanie do tego wyrazu przedrostka „cyber" kreuje termin, który oddaje problematykę podjętą przez Doktoranta w tym rozdziale. Przedmiotem tej części badań jest więc wykorzystanie obowiązujących norm prawa międzynarodowego do wymuszenia określonego rodzaju działania lub zaniechania na stronie konfliktu. Trudno się nie zgodzić z Doktorantem, że jest to zjawisko, które państwa powinny brać pod uwagę przy kształtowaniu własnych polityk w tym zakresie (s. 6). Rozdział piąty rozpoczyna się od analizy pojęcia „lawfare", po to by przejść do zastosowania „cyberlawfare" w operacjach cyberprzestrzennych. Warto zwrócić uwagę, że w kontekście tego problemu działania mogą być prowadzone nie tylko przez podmioty państwowe. Dlatego należy docenić uwzględnienie przez Autora możliwej działalności aktorów niepaństwowych.

Reasumując, w zakresie merytorycznym rozprawa mgra Tomasza Welanyka zasługuje na ocenę pozytywną. Autor precyzyjnie formułuje wnioski naukowe, z którymi na ogół należy się zgodzić, i które znajdują potwierdzenie w cytowanej literaturze, materiałach badawczych oraz w stanowisku doktryny.

Jednocześnie należy podkreślić, że większość omawianych w rozprawie zagadnień nie rodzi większych wątpliwości czy uwag krytycznych. Warto zauważyć, że praca jest wynikiem dogłębnej analizy popartej trafnie dobraną literaturą, analizą przypadków oraz analizą orzecznictwa i praktyki międzynarodowej w zakresie cyberprzestrzeni. Autor rzetelnie porusza się po obszarze badawczym wyznaczonym ramami tematu, trafnie podsumowując stosowne części rozważań.

3. Ocena formalnej strony rozprawy doktorskiej

Wszystkie elementy rozprawy doktorskiej są, co do zasady, prawidłowo sporządzone pod względem formalnym. Bibliografia także nie rodzi wątpliwości. Doktorant zawarł w niej literaturę przedmiotu, wykaz źródeł prawa krajowego oraz źródeł prawa międzynarodowego, a także orzecznictwa. Przypisy zostały sporządzone prawidłowo, a praca nie rodzi wątpliwości od strony formalnej. Ponadto, rozprawa napisana jest poprawną polszczyzną.

4. Konkluzja oceny rozprawy doktorskiej

Po zapoznaniu się z rozprawą doktorską mgra Tomasza Welanyka pt. Istnienie i granice suwerenności w cyberprzestrzeni. Analiza prawna, napisanej pod opieką naukową prof. UEK dra hab. Pawła Czubika (promotora) oraz dra Pawła Filipka (promotora pomocniczego), stwierdzam, że stanowi ona oryginalne rozwiązanie problemu naukowego oraz wykazuje ogólną wiedzę teoretyczną kandydata w dziedzinie nauk społecznych w zakresie nauk prawnych oraz umiejętność samodzielnego prowadzenia pracy naukowej. Oznacza to, iż rozprawa ta spełnia wszystkie wymogi, określone 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 (Dz. U. z 2017 r., poz. 1789), który stosowany jest zgodnie z art. 179 ust. 2 ustawy z dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r., poz. 1669). Tym samym może ona stanowić podstawę do przeprowadzenia dalszych czynności w przewodzie doktorskim, w tym do nadania stopnia naukowego doktora nauk społecznych w zakresie nauk prawnych. Wobec powyższego rekomenduję przyjęcie rozprawy i dopuszczenie mgra Tomasza Welanyka do publicznej obrony rozprawy doktorskiej.