Katowice, dnia 8 maja 2017 roku

Dr hab. Jacek Barcik
Katedra Prawa Międzynarodowego Publicznego i Prawa Europejskiego,
Wydział Prawa i Administracji
Uniwersytetu Śląskiego

Recenzja rozprawy doktorskiej
Mgr Joanny WORONA
pt. *„Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy”*,
Białystok 2017, ss. 622,
przygotowanej pod kierunkiem dr hab. Macieja PERKOWSKIEGO, prof. UwB

I. Ocena wyboru tematu

Jak zauważa Doktorantka we wstępie do dysertacji „według danych witryny Internet World Stats w grudniu 2016 roku liczba internautów przekroczyła 3,6 miliarda. Oznacza to, że aż 49,2% światowej populacji jest częścią globalnej wioski, położonej w nowej przestrzeni o wirtualnym, trangranicznym, aterytorialnym i ponadnarodowym charakterze. Jeszcze nigdy w historii naszego globu nie było możliwości tak łatwego, taniego i szybkiego przesyłania danych czy komunikowania się na odległość”. Warto dodać, że biorąc pod uwagę dotychczasowe trendy liczby te będą zapewnie nadal się zwiększać. Tym samym, obok realnego, pojawia się ściśle z nim sprzężony świat wirtualny, ogarniający coraz więcej dziedzin życia ludzkiego. To już nie tylko komunikacja i przepływ idei, ale także wymiarze komercyjnym e-handel. Zjawiska te, obok niewątpliwych pozytywów rodzą niestety także odpowiadające im niepożądane efekty, jak rozwój cyberprzestępczości, czy cyberterroryzmu. Jest to szerokie spectrum zagadnień, które jedynie w części mają aspekt prawny, w większości bowiem przynależą do sfery zjawisk społecznych i kulturowych. Nawet jednak w dziedzinie prawa, problematyka ta cechuje się interdyscyplinarnością, łącząc kwestie zaliczane do podstawowych gałęzi praw (cywilnego, karnego, administracyjnego). Ponieważ sieć wirtualna nie zna granic państwowych kluczowe dla rozwoju prawa cyberprzestrzeni są regulacje prawa międzynarodowego. Wyłania się w związku z tym szereg pytań związanych tak z aktualnym stanem regulacji *ius gentium* w zakresie cyberprzestrzeni, jak i możliwości wykorzystania powyższego systemu prawa jako instrumentu kreowania pożądanych rozwiązań prawnych w omawianym zakresie. Z tej perspektywy temat wybrany przez

Autorkę jawi się jako niezwykle aktualny, ważny dla nauki, jak i utylitarystycznie przydatny dla stosujących prawo. W pełni spełnia on kryteria wyboru tematu rozprawy doktorskiej

II. Struktura rozprawy

Imponująca objętościowo dysertacja (622 ss.) obejmuje trzy powiązane ze sobą części, w skład których wchodzi sześć rozdziałów. Część I („Cyberprzestrzeń a jurysdykcja") zawiera dwa rozdziały (rozdział 1 „Cyberprzestrzeń – pojęcie i geneza"; rozdział 2 „Jurysdykcja państwowa i cyberprzestrzeń"). W skład części II („Prawnomiędzynarodowy wymiar cyberprzestrzeni – status quo") wchodzi rozdział 3 („Identyfikacja regulacji prawnych cyberprzestrzeni z perspektywy międzynarodowej") i 4 („Identyfikacja kluczowych zagadnień przedmiotowych prawnomiędzynarodowej regulacji cyberprzestrzeni"). Postulować należałoby dodanie do tytułu rozdziału 3 słowa „źródeł", gdyż koncentruje się on na wskazaniu aktualnego stanu prawnego. Ostatnia, III cześć pracy („Koncepcja rekonstrukcji statusu prawnego cyberprzestrzeni (z wykorzystaniem prawa międzynarodowego)") obejmuje dwa rozdziały: 5 („Identyfikacja obszarów regulacji prawnomiędzynarodowych możliwych do wykorzystania rekonstrukcyjnego wobec cyberprzestrzeni"; *nota bene* bardziej niż rekonstrukcja oznaczająca odnowienie, odtworzenie, zasadne byłoby użycie słowa „kreacja", jako że stworzenie ładu prawnego cyberprzestrzeni jest, co zauważa sama Autorka, zadaniem *pro futuro*); 6 („Postulaty i propozycje rozwiązań prawnych dla cyberprzestrzeni"). Powyższa struktura dysertacji jest ze wszech miar właściwa – w części I bowiem Autorka wskazuje na deterytorializację cyberprzestrzeni i problemy z określeniem prawa właściwego, co stanowi wstęp do rozważań dotyczących prawa międzynarodowego, przy czym część druga obejmuje wnioski *de lege lata*, zaś część trzecia *de lege ferenda*. Pracę wzbogacają liczne tabele przystępnie ilustrujące tok wywodu.

Rozdział 1 rozprawy zawiera definicję cyberprzestrzeni oraz genezę i ewolucję tego fenomenu. Autorka wychodzi poza zakres wyznaczony tematem rozdziału, opisując w dalszej kolejności etapy rozwoju społeczeństwa informacyjnego i zagrożenia w cyberprzestrzeni. Słusznie zauważa, że „pojęcie cyberprzestrzeni nie ma jednej, ogólnie przyjętej i akceptowalnej definicji", co „Ze względu na swój dynamicznie zmieniający się, nieostry i niematerialny charakter prowadzi do trudności zarówno interpretacyjnych, jak i definicyjnych" (s. 23). Bardzo trafnie stwierdza także, że „Cyberprzestrzeni nie można utożsamiać z Internetem. Ma ona szerszy charakter, jest przestrzenią cyfrowej działalności człowieka, lecz w dużej mierze bazuje właśnie na sieci Internet" (s. 25). Szczególnie ciekawe

w tym rozdziale pozostają rozważania dotyczące zarządzania Internetem i rozwoju społeczeństwa cyfrowego. W pierwszym przypadku Autorka trafnie wymienia dwie podstawowe cechy cyberprzestrzeni: decentralizację („Zarządzenie nim (Internetem – JB. przypomina system feudalnych władztw terytorialnych – każdy podmiot administruje własną (najczęściej stworzoną przez siebie) częścią tej struktury oraz pokrywa związane z tym wydatki. Zdecentralizowana struktura stanowienia i egzekwowania reguł postępowania jest jedną z najważniejszych cech charakterystycznych, z punktu widzenia prawnej analizy tego fenomenu" (s. 26) i; substrat społeczny („Stopniowo wzrasta siła jednostki, słabnie natomiast przywiązanie do osadzonego na fundamencie terytorialnym państwa", s. 27). Doktorantka podziela pogląd, że ten ostatni doprowadził do wykształcenia się społeczeństwa informacyjnego w którym, co należy uznać za nazbyt optymistyczny wniosek, wiedza i informacja jest priorytetem (s. 22-23). Za P. Sienkiewiczem wymienia także warianty rozwoju społeczeństwa informacyjnego (s. 59). Rozważania w powyższych punktach stanowią ciekawy przyczynek do analizy szerszego problemu ewolucji samego prawa międzynarodowego (od klasycznego państwowocentrycznego „international law" do spluralizowanego „global law") oraz jego fragmentacji. Materia ta wykracza także poza nauki prawne, wkraczając w obszary zarezerwowane dla innych nauk społecznych, o czym świadczy funkcjonowanie, przypisywanego Umberto Eco, podziałowi społeczeństwa informacyjnego na trzy klasy: digitariat, cogitariat i proletariat. Najwyższa z wymienionych klas – digitariat, jest zarówno konsumentem, jak i kreatorem globalnej sieci. Wiąże się z tym zjawisko tak wykluczenia, jak i uprzywilejowania sieciowego.

Rozdział 2 analizuje kwestie jurysdykcyjne w odniesieniu do cyberprzestrzeni. Warto byłoby zawrzeć w jego ramach zdanie wyjaśnienia, czy pojęcia „jurysdykcja" i „właściwość" są pojęciami tożsamymi. W ramach powyższego rozdziału wyraźnie odróżniają się dwie części: jedna poświęcona jurysdykcji cywilnej, druga zaś karnej. Są one badane w ujęciu globalnym, regionalnym i krajowym, prawnoporównawczym. W rozdziale tym pojawiają się po raz pierwszy, obecne także w kolejnych częściach pracy nieponumerowane, nie ujęte w spisie treści podrozdziały (np. ss. 82, 87, 89, 94, 100, 102, 103, 107, 111, 115, 117, 118, 124, 128, 130 itd.). Rozumiem, że są to jednostki opisu wewnętrznego na użytek pracy i nie stawiam zarzutu z tego powodu, niemniej jednak w razie publikacji pracy należałoby je uwzględnić w spisie treści. Część poświęcona jurysdykcji cywilnej dowodzi ogromnej wiedzy Autorki w zakresie prawa międzynarodowego prywatnego i mogłaby być odrębnym studium w tym zakresie (np. ciekawe uwagi dotyczące *forum shopping* w zakresie jurysdykcji – s. 76).

Ciekawa jest identyfikacja przyczyn sporów kompetencyjnych w cyberprzestrzeni, w pełni zgadzam się także ze stanowiskiem Autorki (wyrażonym za A. Całusem), że „Wprowadzenie więc zunifikowanego systemu odpowiedzialności cywilnej uzależnione jest poniekąd od wcześniejszego ujednolicenia zasad jurysdykcji karnej" (s. 76). Doktorantka omawia poszczególne konwencje międzynarodowe z zakresu prawa międzynarodowego prywatnego, rozważając ich zastosowanie do cyberprzestrzeni. Warto jednak zauważyć, że nie wszystkie państwa są ich stronami, co powoduje, że możliwość ich zastosowania do sfery cyberprzestrzeni zawsze będzie ograniczona. Z analizy wyłania się ogólna konkluzja, że sądem właściwym do rozpoznania sprawy będzie z reguły sąd miejsca zamieszkania lub siedziby pozwanego. Doktorantka nie wyjaśnia jakimi kryteriami kierowała się przy wyborze państw do analizy komparatystycznej (ich lista w zakresie jurysdykcji cywilnej nie pokrywa się z kluczem przyjętym w zakresie jurysdykcji karnej), niemniej wywody w tym zakresie są niezwykle interesujące, okraszone orzecznictwem i poglądami krajowej doktryny. Pewien mój drobny niedosyt wzbudza jedynie nieproporcjonalność wywodów (np. obszerna na kilku stronach analiza dotycząca Francji, i, skąpa wzmianka o regulacjach niemieckich i brytyjskich – zaledwie pół strony – s. 102). Polska jest opisana w zakresie regulacji jurysdykcji karnej, natomiast pominięta przy jurysdykcji cywilnej. W razie publikacji rozprawy warto byłoby uzupełnić ją o wskazanie trudności związanych z dochodzeniem odpowiedzialności w przypadku deliktów w cyberprzestrzeni. Czy przypisanie takiej odpowiedzialności może nastąpić na podstawie identyfikacji adresu IP (Internet Protocol)? Czy nie narusza to zasady indywidualizacji odpowiedzialności?

Rozdział 3 identyfikuje regulacje prawne dotyczące cyberprzestrzeni. Dominuje podejście instytucjonalne, a nie przedmiotowe. Doktorantka bada w pierwszej kolejności regulacje wypracowane na forum ONZ (w tym organów pomocniczych organizacji) oraz w systemie ONZ (WIPO, ITU). W wymiarze regionalnym opisany jest dorobek Rady Europy i Unii Europejskiej. Autorka zasadnie podkreśla znaczenie pierwszej z wymienionych organizacji, w ramach które przyjęto, szeroko komentowaną, Konwencję o cyberprzestępczości z 2001 r. Jest to, co trafnie stwierdza Autorka najistotniejszy akt prawny o charakterze międzynarodowym odnoszący się do zagadnienia przestępczości popełnianej przy użyciu systemów komputerowych. Są nim związane także państwa spoza systemu Rady Europy. Ciekawym byłoby zatem zbadanie, czy przyjęte w nim rozwiązania nadają się do recepcji na szczebel uniwersalny. Autorka jedynie enigmatycznie wspomina, że rozwiązanie przyjęte w konwencji wydają się obecnie przestarzałe (s. 198). Opisując dorobek organizacji

wyspecjalizowanych Doktorantka zalicza do nich m.in. dorobek Europejskiej Agencji Bezpieczeństwa Sieci i Informacji. Zabieg taki z perspektywy prawa międzynarodowego może wydawać się uzasadniony, jednak z perspektywy prawa UE kwalifikowanie agencji jako organizacji wyspecjalizowanych jest błędne (pozostają one z reguły jednostkami organizacyjnymi UE pomocniczymi względem instytucji – najczęściej Komisji Europejskiej). Bardzo ciekawe i cenne, a niekiedy wręcz pionierskie w nauce polskiej, są rozważania dotyczące polityki cyberbezpieczeństwa NATO (S. 247-248), Darknetu (s. 261) i regulacji krajowych (np. Chin w kontekście ustawy Great Firewall – s. 300), dorobku grupy G8 (s. 267) i Brytyjskiej Wspólnoty Narodów (s. 268).

Rozdział 4 zawiera kompetentne studiów praktycznych problemów związanych ze prawnomiędzynarodową represją w cyberprzestrzeni. Doktorantka bada zarówno zagadnienia karne (cyberprzestępstwa przeciwko bezpieczeństwu elektronicznie przetwarzanej informacji; Naruszenie integralności danych komputerowych i systemu komputerowego; cyberprzestępstwa przeciwko mieniu; cyberprzestępstwa związane z treścią informacji; kradzież tożsamości w cyberprzestrzeni; cyberterroryzm), jak i kwestie obrotu gospodarczego (w tym zawieranie umów w cyberprzestrzeni; elektroniczne środki płatnicze), własności intelektualnej, ochrony danych osobowych. Rzetelnie zrekonstruowano problemy w zwalczaniu cyberprzestępczości (s. 322), wskazano źródła zagrożeń, zdefiniowano tak istotne kwestie jak m.in. sabotaż komputerowy (w tym rodzaje wirusów), oszustwo komputerowe, fałszerstwo komputerowe, *phishing, pharming., cyberstalking, grooming*. Doktorantka definiuje także umowę elektroniczną (s. 384) i sposoby jej zawierania. Nie pominięto kwestii *bitcoinów* (s. 438), piractwa internetowego, czy własności intelektualnej w kontekście chmury obliczeniowej (s. 454). W zakresie ochrony własności intelektualnej brakuje, co warto byłoby uzupełnić w przypadku publikacji rozprawy, wzmianki o pionierskich francuskich regulacjach zawartych w ustawie HADOPI z 2009 r. (*Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet – Wysoki urząd ds. rozpowszechniania utworów i ochrony praw w Internecie*). Organ ten mógł z mocy prawa po wystosowaniu dwóch ostrzeżeń, przy trzecim stwierdzeniu naruszenia praw autorskich, zdecydować o odcięciu użytkownikowi dostępu do Internetu. Warto także wspomnieć o dwóch podstawowych koncepcjach ochrony praw własności intelektualnej w Internecie: koncepcji *graduate response* i *notice and take down*. Pewien niedosyt wzbudza u mnie podrozdział 4.4.1. zatytułowany „Cyberprzestrzeń a prawa", w którym Autorka zajmuje się prawem do prywatności i ochroną korespondencji. W ogóle nie wspomina o kształtowaniu się prawa dostępu do Internetu jako prawa człowieka.

Uznanie normatywnego charakteru tego prawa determinuje uznanie adekwatnych pozytywnych obowiązków państw, co ma zasadnicze znaczenie dla ludzkiej aktywności w sieci elektronicznej. Autorka mogła omówić to zagadnienie już na samym początku rozprawy.

W rozdziale 5, indyferentnym z perspektywy celów pracy, ale służącym do zilustrowania dalszych wywodów, Doktorantka omawia subreżimy prawne międzynarodowego prawa morza, przestrzeni kosmicznej i antarktyczny (podrozdział 5.2. „Prawo międzynarodowe wobec przestrzeni"). W dalszej kolejności w niezbyt jasno zatytułowanym podrozdziale „Prawo międzynarodowe jako law in action" (podrozdział 5.3) opisane zostają ochrona klimatu i kosmos, przy czym w przypadku tego ostatniego niepotrzebnie podzielono rozważania z pkt. 5.2 wywodów. Rozdział 5 służy jako wprowadzenie do ostatniej części pracy, w której Doktorantka zawiera postulaty i propozycje rozwiązań prawnych dla cyberprzestrzeni. Jest to rozdział w dużej części analityczny i, jak dla mnie, najważniejszy i najciekawszy spośród wszystkich części recenzowanej, interesującej dysertacji. Analizie podlegają koncepcje samoregulacji cyberprzestrzeni, w tym koncepcja *lex informatica*, uznanie cyberprzestrzeni za czwartą przestrzeń międzynarodową, czy inicjatywa *Creative Commons*. Na tej podstawie Autorka proponuje rozwiązania w zakresie regulacji cyberprzestrzeni w postaci przyjęcia nowej konwencji ramowej. Do swojej propozycji podchodzi jednak z intelektualną pokorą, o czy świadczy rozsądne stwierdzenie, że „Zaproponowane rozwiązanie, ze względu na znaczny obszar regulacji, nie może być uznane za holistyczną i kompletną regulację rozwiązującą wszystkie problemy cyberprzestrzeni, lecz będzie przyczynkiem do dalszej dyskusji nad tym nowym, problematycznym zagadnieniem" (s. 525-526).

Pracę zamyka Podsumowanie (11 ss.).

Resumując, wskazane powyżej uwagi mają charakter w większości techniczny i nie wpływają na ogólną pozytywną ocenę struktury rozprawy. Pozostaje ona zasadniczo klarowna, logiczna i sprzyjająca osiągnięciu postawionych celów badawczych.

III. Tezy rozprawy i metodologia badań

Doktorantka bardzo szeroko zakreśliła cel rozprawy, zaliczając do niego tak „weryfikację aktualnego statusu prawnego cyberprzestrzeni w kierunku jej optymalnego uregulowania z wykorzystaniem prawa międzynarodowego", jak i dokonanie identyfikacji „obszarów, w których istnieje konieczność unifikacji przepisów odnoszących się do cyberprzestrzeni" (s. 15). Tak szeroko zakreślona materia badawcza jest zrozumiała biorąc

pod uwagę interdyscyplinarny charakter rozprawy, rodzi ona jednak niebezpieczeństwo rozproszenia głównego toku wywodu i „ugrzęźnięcia" w wątkach pobocznych. Lektura rozprawy pozwala jednak stwierdzić, że Doktorantka uniknęła tego zagrożenia, zręcznie i sprawnie koncentrując się na zagadnieniach związanych z tezą rozprawy.

Głównym problemem badawczym zidentyfikowanym przez Autorkę jest ustalenie, czy prawo międzynarodowe może udoskonalić rekonstrukcyjnie aktualny status cyberprzestrzeni. Ujęty w sposób ogólny problem badawczy jest precyzowany przez szereg szczegółowych pytań badawczych sformułowanych przez Doktorantkę. Są to pytania o to: czy cyberprzestrzeń, jako przedmiot regulacji, można ująć definicyjnie?; Jakie reguły jurysdykcyjne są stosowane w stosunku do cyberprzestrzeni?; Czy i w jaki sposób oraz w jakim zakresie państwa, organizacje międzynarodowe i inne podmioty podejmują próby regulacji cyberprzestrzeni?; Czy prawo międzynarodowe umożliwia regulację cyberprzestrzeni?; W jakich płaszczyznach prawo międzynarodowe może mieć zastosowanie w stosunku do cyberprzestrzeni?; W jakich obszarach prawo międzynarodowe przyczynia się do unifikacji problematycznych kwestii związanych z cyberprzestrzenią?; Jakie są najbardziej adekwatne postulaty i propozycje rozwiązań prawnych regulacji cyberprzestrzeni?. Postawione pytania badawcze prowadzą Doktorantkę do sformułowania tezy pracy, zgodnie z którą prawo międzynarodowe jest najbardziej predysponowane do racjonalnego i użytecznego modelowania oraz harmonizacji regulacji krajowych cyberprzestrzeni. Jest to teza logiczna, spójna i niesprzeczna wewnętrznie. Jako taka spełnia wymogi twierdzeń naukowych. Dla jej weryfikacji Doktorantka posługuje się paletą metod badawczych. Metodologia pozostaje mocną stroną dysertacji. Doktorantka już we Wstępie precyzuje przedmiot badań i tezy pracy oraz przyjęte metody badawcze. W dalszych częściach rozprawy konsekwentnie trzyma się przyjętych założeń, odnosząc się do nich w poszczególnych rozdziałach oraz, wieńczącym rozprawę, Podsumowaniu. Autorka stosuje metodę dogmatyczną, która służy Jej do „określenia norm prawnych stosowanych w przestrzeni wirtualnej oraz do identyfikacji przedmiotowych obszarów, w których istnieje potrzeba regulacji i harmonizacji". Wykorzystywana jest także metoda prawno porównawcza, pozwalająca na „poznanie różnorodności obowiązujących regulacji oraz na wyciągnięcie wniosków w zakresie prawidłowości przyjętych rozwiązań". Używana jest również metoda analizy orzecznictwa i doktryny służącą badaniu praktyki sądowej; metoda historyczna konieczna dla przedstawienia genezy regulacji dotyczących cyberprzestrzeni. Wychodząc poza nauki prawne Autorka stosuje metodę analizy statystycznej, dzięki której ilustruje „dynamikę wzrostu liczby

użytkowników cyberprzestrzeni, ilościowy rozwój przestrzeni wirtualnej, rodzaje i liczbę naruszeń występujących w sieci czy też skalę problemów takich, jak *cyberstalking*".

Z pełnym przekonaniem można uznać, że Doktorantce udało się potwierdzić założoną tezę badawczą. W kontekście zarządzania cyberprzestrzenią stawia niezwykle interesujący postulat uznania przestrzeni cyfrowej, za nowe elektroniczne, globalne dobro wspólne. Wykorzystywana być ona powinna „dla wspólnego dobra całej ludzkości, a każdy internauta winien mieć dostęp do zgromadzonych w niej zasobów (wiedzy, informacji, edukacji, rynków zbytu)". Autorka odrzuca zarazem propozycje zarządzania cyberprzestrzenią wyłącznie przez autoregulację, argumentując to faktem, że „oddolny sposób regulacji przestrzeni wirtualnej determinuje zbyt duże ryzyko nadużyć, a brak odpowiedniego autorytetu spowodować może nieefektywność stosowania sankcji w przypadku zachowań niezgodnych z ogólnie przyjętą „netykietą". Jest to argument zasługujący na poparcie, rodzi jednak pytanie kto i jak ma zorganizować system zarządzania cyberprzestrzenią? Doktorantka słusznie i z wyczuciem odpowiada, że „system ten winien być stosowany pomocniczo, w myśl wolnościowego charakteru cyberprzestrzeni. Próby odgórnego narzucenia określonych rozwiązań przez państwa i bagatelizowanie cybernetycznej społeczności mogą doprowadzić do zbiorowych protestów, nie tylko w przestrzeni wirtualnej, lecz również w świecie realnym" (vide umowa ACTA). Zatem „przy braku jasnych regulacji, prawo międzynarodowe winno być (metodologicznie) stosowane rekonstrukcyjnie, by udoskonalać aktualny status cyberprzestrzeni". Jak jednak to osiągnąć? Doktorantka proponuje stworzenie jednego, „centralnego ośrodka międzynarodowego, który miałby kompetencje do tworzenia prawa cyberprzestrzeni". Organ taki „mógłby zostać utworzony jako zupełnie nowa, niezależna instytucja międzynarodowa bądź jako organizacja wyspecjalizowana w ramach ONZ", i „zapewniać reprezentację wszystkich najważniejszych podmiotów międzynarodowych i przedstawicieli społeczeństwa informacyjnego, w tym sektora prywatnego". Zgłaszając powyższy postulat Doktorantka musi zdawać sobie sprawę z faktu, że jego realizacja jest eufemistycznie pisząc problematyczna. System międzynarodowy mimo faktycznych zmian nadal oparty jest o dysponujące atrybutem suwerenności państwa, co oznacza, że nikt nie może zmusić państw do przystąpienia do wspomnianego systemu, zaś uczestnicy pozapaństwowi występowałyby w nim na gorszych prawach, gdyż państwa zazdrośnie strzegą swojego imperium, nawet, jeśli z biegiem czasu przybiera ono postać symboliczną.

W pełni natomiast przekonuje mnie proponowane użycie instrumentu konwencji ramowej jako sposobu na globalną i holistyczną regulację cyberprzestrzeni. Istota konwencji

ramowej polega na przyjęcia podejścia, określanego w nauce amerykańskiej mianem „*framework convention and protocol approach*". Sprowadza się ono do zawarcia ogólnej umowy międzynarodowej z danego zakresu, która następnie jest uzupełniana w drodze protokołów dodatkowych. Strony umowy często zakładają jednak pewien etap instytucjonalizacji współpracy (np. poprzez kreację Konferencji Stron, tworzenie wyspecjalizowanych ciał doradczych), który pozwala na późniejsze opracowywanie protokołów dodatkowych do traktatu i kontrolę jego przestrzegania. Konwencje ramowe są wyrazem intencji stron stworzenia szerszego reżimu regulacyjnego w danej dziedzinie. Jego powstawanie odbywa się w dwóch etapach. W pierwszym przyjmuje się konwencję ramową, mającą ułatwiać przyszłą współpracę i wyrażającą ogólne cele przyszłego reżimu regulacyjnego oraz zobowiązanie stron do uczestnictwa w nim. Jest ona na tyle ogólnie sformułowana, że pozwala państwom zachować pewien margines swobody wynikający m.in. z odmiennych interesów narodowych. W tym sensie konwencja ramowa jest swoistym „parasolem" dla dalszej współpracy, który może znakomicie się sprawdzić w przypadku prawa cyberprzestrzeni. Zarazem wiązanie się protokołami dodatkowymi jest otwarte tylko dla państw związanych konwencją ramową. Ich stosowanie podlega także interpretacji zgodnej z konwencją ramową. Rozwój reżimów regulacyjnych w ramach konwencji zależy zatem od uzgodnień państw w Konferencjach Stron, dlatego niezbędna jest skuteczna dyplomacja w tym zakresie.

Na uznanie zasługuje fakt, że Doktorantka dostrzega potencjał norm *soft law* dla budowy prawa cyberprzestrzeni. Normy takie stanowią często wstęp do późniejszego przyjęcia instrumentów prawa „twardego". Mają one szereg zalet, pozwalających ominąć mankamenty tradycyjnego prawa konwencyjnego, tj.: a) obowiązują na zasadzie milczącej zgody, co eliminuje problem braku woli politycznej do przyjęcia normy *hard law*; b) mają krótszy okres czasu kreacji w porównaniu z normą *hard law*, co pełni niebagatelną rolę w przypadku dynamicznie rozwijających się technologii internetowych. W procesie jej tworzenia brak jest np. długotrwałej procedury ratyfikacyjnej charakterystycznej dla umów międzynarodowych zawieranych w trybie złożonym. W tym sensie norma *soft law* jako instrument znacznie bardziej elastyczny często lepiej niż tradycyjna umowa odpowiada na potrzeby i wyzwania związane z globalnym zarządzaniem; c) wypełniają lukę regulacyjną w określonej dziedzinie; d) mogą być adresowane do uczestników stosunków międzynarodowych nie będących podmiotami prawa międzynarodowego.

Reasumując, ocena rozprawy dotycząca sformułowania i realizacji założonej przez Doktorantkę tezy badawczej oraz przyjętej metodologii wypada dla Niej wyjątkowo pozytywnie.

IV. Warsztat naukowy

Jak zauważyłem w poprzednich punktach recenzji praca jest niezwykle obszerna (622 ss.), co w pierwszym momencie może być przytłaczające dla czytelnika, a zwłaszcza dla recenzenta. Jest to skutek podejścia Doktorantki, która ambitnie podjęła się próby kompleksowej analizy całego spectrum zagadnień wiążących się z cyberprzestrzenią. Pojawia się pytanie, czy w obecnej dobie dynamicznego rozwoju technologicznej jest to jeszcze w ogóle możliwe? Ponadto tak duża objętość dysertacji rodzi ryzyko rozproszenia celów pracy oraz ugrzęźnięcia w pobocznych dla tematu wątkach. Aby temu zapobiec, konieczne jest wykazywanie się umiejętnością syntezy, koncentrowania się na zagadnieniach istotnych. Jest to ważny probierz oceny warsztatu naukowego. Z satysfakcją muszę stwierdzić, że Doktorantka dobrze zdaje powyższy egzamin. Oczywiście w pracy zdarzają się partie tekstu irrelewantne z perspektywy tezy pracy (taki charakter mają m.in. podrozdziały 5.1. „Specyfika prawa międzynarodowego"; 5.2. „Prawo międzynarodowe wobec przestrzeni"; 5.3. „Prawo międzynarodowe jako law in action"). Nie determinują one jednak ogółu treści rozprawy, która pozostaje przemyślana i dopasowana do założonej tezy. Często także pozornie niezwiązane z tematem rozważania (jak np. pkt. 5.2.2.1 „Morze otwarte oraz dno mórz i oceanów") służą, co okazuje się w dalszych częściach pracy do dokonywania interesujących analogii ze sferą cyberprzestrzeni. Zabieg taki jest niewątpliwie zamierzony przez Autorkę.

Praca cechuje się wysokim poziomem merytorycznym. Autorka poprawnie, zgodnie z zasadami logicznego rozumowania wyciąga wnioski z przeprowadzonych badań. Oryginalny pod tym względem jest zwłaszcza końcowy, szósty rozdział pracy „Postulaty i propozycje rozwiązań prawnych dla cyberprzestrzeni". Pozostaje on dla mnie najciekawszą częścią rozprawy, która nie byłaby jednak możliwa bez przeprowadzenia rozważań w poprzedzających rozdziałach. Niezwykle cenny jest wniosek Doktorantki dotyczący roli partnerstwa publiczno – prywatnego w budowie bezpieczeństwa cyberprzestrzeni) (s. 565). Konkluduje, że tworzenie bezpieczeństwa cyberprzestrzeni nie może odbyć się bez partnerstwa publiczno-prywatnego (szczególnie w obszarze infrastruktury krytycznej w

zakresie współpracy z prywatnymi firmami z branży energetycznej, paliwowej, powietrznej, finansowej) oraz ścisłej współpracy z podmiotami prywatnymi.

Wywód prowadzony jest przez Doktorantkę w sposób rzetelny i uporządkowany, solidnie bazując na poprawnie cytowanej, szerokiej bazie bibliograficznej. Wykorzystana literatura obejmuje tak pozycje polskojęzyczne, jak i obcojęzyczne (w języku angielskim ale także francuskim). Dla ich zebrania Doktorantka odbyła kwerendy w Bibliotece Parlamentu Europejskiego, Bibliotece Uniwersytetu w Antwerpii oraz w Bibliotece przy siedzibie Międzynarodowego Trybunału Sprawiedliwości w Hadze. Szeroko wykorzystywane są także judykaty, tak sądów międzynarodowych, jak i krajowych.

Język jakim operuje Doktorantka świadczy zasadniczo o dobrym opanowaniu warsztatu naukowego. Niezmiernie rzadko pojawiają się tu uwagi krytyczne. Doktorantce zdarzają się bowiem skróty myślowe (np. s. 273 – „nie do końca jawne militarne cyberjednostki"), błędy logiczne (s. 147 – „miliony kilometrów") i błędy literowe (ss. 35, 36, 88).

Podsumowując, warsztat naukowy Autorki pozostaje na wysokim poziomie. Doktorantka jest metodologicznie przygotowana do prowadzenia badań naukowych i posiada umiejętność właściwej selekcji źródeł.

V. Konkluzja

Recenzowana rozprawa stanowi oryginalne rozwiązanie problemu naukowego, pozwala także stwierdzić ogólną wiedzę teoretyczną Doktorantki w zakresie prawa oraz opanowanie przez nią umiejętności samodzielnego prowadzenia pracy naukowej. Tym samym spełnia wymagania określone w art. 13 ust. 1 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (Dz.U. 2003 Nr 65, poz. 595), jakim powinny odpowiadać prace doktorskie. Na uwagę zasługuje pionierski w nauce polskiej i interdyscyplinarny charakter pracy. **Biorąc powyższe pod uwagę wnoszę o dopuszczenie rozprawy do publicznej obrony. Jednocześnie, zważywszy na wysokie walory naukowe dysertacji wnoszę o wyróżnienie rozprawy.**

Dr hab. Jacek Barcik