dr hab. Wiesław Jasiński, prof. WSPol
Wydział Bezpieczeństwa Wewnętrznego
Wyższa Szkoła Policji

Szczytno, 6.11.2017

Recenzja rozprawy doktorskiej mgr. Janusza Konrada Wasilewskiego pt. *Cyberprzestępczość – wybrane aspekty prawnokarne oraz kryminalistyczne*, napisanej pod kierunkiem dr. hab. Ewy M. Guzik-Makaruk, prof. UwB w Katedrze Prawa Karnego Wydziału Prawa Uniwersytetu w Białymstoku

I. Uwagi wstępne

W związku z powołaniem mnie w dniu 26 września 2017 r. przez Radę Wydziału Prawa Uniwersytetu w Białymstoku na recenzenta w przewodzie doktorskim mgr. Janusza Konrada Wasilewskiego przedstawiam ocenę rozprawy doktorskiej pt. *Cyberprzestępczość – wybrane aspekty prawnokarne oraz kryminalistyczne* napisanej pod kierunkiem dr. hab. Ewy M. Guzik-Makaruk, prof. UwB. Celem oceny jest ustalenie czy ta rozprawa doktorska spełnia wymogi przewidziane w art. 13 ust. 2 ustawy z dnia 14 marca 2004 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U z 2014 r., poz. 1852 z późn. zm.).

II. Wybór tematu rozprawy doktorskiej oraz ocena jej płaszczyzny formalno-redakcyjnej

1. Temat rozprawy został wybrany trafnie. Jest on ważny w wymiarze praktycznym i naukowym. Jego aktualność wynika głównie z pilnej potrzeby uwzględniania przestępnego ingerowania w dynamicznie rozwijający się świat

wirtualny w obszarze funkcjonowania prawa w płaszczyźnie materialnej i procesowej. Autor odnotowuje stan deficytu *...artykułów oraz opracowań poruszających tę tematykę.* Twierdzi, w tym kontekście, że *...opracowania często przybierają postać wysoce fragmentaryczną, zaś prowadzone rozważania prawnicze najczęściej opierają się na analizie dogmatycznej przepisów, nie wnikając w stronę merytoryczną zjawiska (brak kontekstu faktycznego). Jednocześnie, opracowania tematu starsze niż zaledwie 3-4 lata pozostają obecnie już w dużej mierze nieaktualne z uwagi na zachodzące zmiany zjawiska przestępczości cybernetycznej* (cytat za Autorem: s. 9).

Autor dokonał wyboru tematu nie bez małych problemów proponując ujęcie w tytule także zagadnień kryminologicznych. Faktycznie rozprawa obejmuje przede wszystkim aspekty prawnokarne. Poza tym, w znacznej części Autor skupia się także na problematyce kryminalistycznej i jej poświęca bardzo profesjonalnie rozdział piąty i szósty dysertacji. Jednocześnie wskazać należy, że poszczególne części pracy obejmują także zagadnienia kryminologiczne. Wydaje się, że w kontekście rozterek Autora, ale też po analizie rozprawy najtrafniej byłoby wybrać tytuł: „Cyberprzestępczość – wybrane aspekty prawnokarne, kryminologiczne i kryminalistyczne". Każdy z tych aspektów jest bowiem reprezentowany w rozprawie mgr. Janusza Wasilewskiego.

2. Rozprawa doktorska mgr. Janusza Wasilewskiego ma, dopuszczoną przez art. 13 ust. 2 ustawy z dnia 14 marca 2004 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz.U z 2014 r., poz. 1852 z późn. zm.) formę maszynopisu książki i liczy (ponumerowanych od spisu treści) 428 stron. Dzieło obejmuje wstęp, sześć rozdziałów, wnioski i bibliografię. W konstrukcji dysertacji daje się wyodrębnić trzy części. Pierwszą stanowi charakterystyka pojęcia i zakres cyberprzestrzeni oraz składających się nań technologii (rozdział II i III). Druga obejmuje systematykę oraz kwalifikację prawną wybranych cyberprzestępstw (rozdział IV) ale też genezę regulacji prawnych w obszarze zapobiegania i

zwalczania przestępstw w cyberprzestrzeni (rozdział I). Wreszcie część trzecia dotyczy ujęcia procesowego problematyki rozprawy i obejmuje rozdział V (*Dowód elektroniczny – charakterystyka oraz klasyfikacja śladów cyberprzestępstw*) oraz rozdział VI (*Transpozycja czynności procesowych do obszaru cyberprzestrzeni*). Wydaje się, że w przyjętej konstrukcji możliwe było umieszczenie rozdziału I jako poprzedzającego rozdziały IV, V i VI. Obejmuje on bowiem problematykę obu kategorii regulacji (materialnoprawnych i prawnoprocesowych) charakteryzowanych w części drugiej i trzeciej Dzieła. Autor zamierzał, co słuszne, potraktować rozdział I jako swoiste wprowadzenie do trzech części, o których mowa wcześniej ale efektu tego nie osiągnął przynajmniej z dwóch powodów. Po pierwsze, w § 1 (*Uwagi ogólne*) powtarza kwestie, które w innym ujęciu podejmuje także we wstępie. Po drugie, w § 2 prezentuje już tylko kwestie genezy regulacji (*Geneza regulacji*) a tym samym daje argumenty do zaproponowania innej chronologii jednostek redakcyjnych. Odnotować należy też pewne zachwianie proporcji zawartości rozdziału I - § 1 obejmuje 5 stron a § 2 – stron 15. Tym bardziej jest to istotne, że są to jedyne jednostki tego rozdziału a tytuł drugiej z nich jest w pewnym sensie powtórzeniem tytułu całego rozdziału.

3. We wstępie Autor formułuje problemy (ogólne i szczegółowe) i hipotezy badawcze (ogólne i szczegółowe). Umiejscawia je w sześciu odcinkach. Pozwala to czytelnikowi na precyzyjne podążanie za wywodami. Autorowi z kolei pozwala zachować reżim koncepcyjny w całej rozprawie.

4. Autor konstruuje trzy kategorie wniosków: w zakresie definicji cyberprzestrzeni (ss.406 – 412), w zakresie regulacji zjawiska cyberprzestępczości (ss. 412-417), w zakresie transpozycji czynności procesowych do obszaru cyberprzestrzeni (ss. 417-422). W pierwszej grupie wnioski w znacznej części *de facto* są kopiowaniem tych, które pojawiają się na zakończenie treści rozdziału II. Takie

ujęcie ma służyć Autorowi do konstruowania postulatów prawnych odnoszących się do sposobu legalnego postrzegania domeny cyfrowej. Niestety w tym zakresie katalog wydaje się nader ubogi. *De facto* uwagę zwraca jedynie postulat uporządkowania przepisów pod kątem stosowanej w nich siatki pojęciowej, tak by każda z ustaw branżowych posługiwała się jednolitym, wspólnym aparatem pojęciowym (s. 410) oraz postulat konieczności przyjęcia do polskiego prawa definicji pojęcia „cyberprzestrzeń" (s.412). Pozostałe wnioski i postulaty z powodzeniem umiejscowić można w drugiej części (zakres regulacji zjawiska cyberprzestępczości) lub trzeciej (zakres transpozycji czynności procesowych do obszaru cyberprzestrzeni). Zresztą Autor sam na s. 411 wskazuje, że wniosek dalej będzie rozszerzony. Wydaje się, że takie ujęcie jest niewłaściwe dla podsumowania pracy. Część drugą i trzecią wniosków ujęto w sposób, który świadczy o wybitnym znawstwie materii i ich zakres jest sam w sobie wartością dodaną w tej kategorii badawczej.

5. Autor zdecydował, że podsumuje poszczególne rozdziały wynikami badań. Wykazuje tym samym umiejętność syntetycznego ujmowania materii badawczej. Znaleźć można zatem podsumowanie rozdziału I, II, III, VI i niezwykle krótkie – rozdziału V (ss. 330-331). Nie jest w tej kwestii jednak konsekwentny - podsumowania nie zawiera bardzo ważny dla całej rozprawy rozdział IV.

6. Rozprawa jest objętościowo bardzo obszerna. W jej konstrukcji można zaproponować pewne rozwiązania ułatwiającą lekturę, np. można to przeprowadzić w procesie redakcyjnym przed publikacją, którą niewątpliwie zalecam. Dla przykładu, konieczny byłby podział jednostek redakcyjnych niższego rzędu, np. w rozdziale IV w § 2 wyodrębniono pkt. 4: *Zamieszczanie w cyberprzestrzeni materiałów zabronionych prawem;* w nim wyodrębnia się jeszcze kilka części ale nie posiadają one żadnej numeracji. Tym samym nie można odnaleźć owej zawartości w spisie treści.

Inny przykład to dowolne stosowanie przez Autora formy wprowadzenia do rozdziałów bez odpowiedniej sygnalizacji tego elementu konstrukcyjnego pracy.

7. Odrębnie należy odnieść się do kwestii terminologicznej. Autor stosuje mnóstwo pojęć technicznych, które umiejętnie definiuje. Zachowuje reżim terminologiczny w sposób godny podziwu i w pełni profesjonalny. Jednakże pewien element tej płaszczyzny rozprawy wymaga komentarza. Otóż zamiennie Autor stosuje termin „przestępstwo cybernetyczne" i „cyberprzestępstwo". Tymczasem w literaturze trwa istotna dyskusja w tym zakresie i zdaje się, że krystalizuje się bardzo ważny pogląd, zgodnie z którym wyprowadzanie przedrostka „cyber-„ od słowa „cybernetyka" nie jest uprawnione. Szkoda, że Autor nie odnosi się do tej ważnej kwestii terminologicznej.

8. Język Autora jest precyzyjny i prawniczo fachowy. Konstrukcje zdań są logiczne i poprawne, co dla prezentacji skomplikowanej materii jest bardzo ważne. Nie znaczy to jednak, że Autor nie ustrzegł się wielu wadliwości językowych.

Niewłaściwie używa niektórych wyrazów, określeń czy zwrotów, np. *„najświeższej historii"* (powinno być: najnowszej, s. 26) czy: *„...problematyczność stosowania do przedmiotowego problemu..."* (s.365).

Kilka błędów uznać można za poważne. Zakładam, że o swojej osobie powinno pisać się z małej litery, tymczasem Autor używa, niestety nieprzypadkowo, bo w bardzo wielu miejscach literę dużą – Autor, np. s. 165, s. 166, s. 208. Zbyt często w rozprawie zdania rozpoczynają się od słowa „ponieważ", np. s. 209 czy s. 198. Kilkakrotnie Autor używa dużej litery dla przymiotników geograficznych, np. *obywatelowi Angielskiemu* – s. 420; *administrację Niemiecką* – s. 354; *prawodawca Unijny* – s. 225 czy *ustawodawca Polski* – s. 225. Istotnym błędem w języku prawniczym jest pisany skrótem na początku zdania *„art."*, np. s. 224 czy s. 276 oraz w bardzo wielu innych miejscach. Autor używa też dużej litery dla słowa internauta, co

językoznawcy uważają za błędne – s. 224. Różnie też pisany jest *hacktywizm*, np. *haktywizm* – s. 224.

Autor przesadnie często odwołuje się do wcześniejszych treści swojej rozprawy albo zapowiada następne wątki. Tym samym daje dowód panowania nad ogólnym przekazem i wykazuje samodzielność wywodu ale w żaden sposób nie ułatwia to lektury. Wręcz przeciwnie komplikuje ją, w szczególności gdy jest to powoływanie się natarczywe. Dla przykładu, tylko na s. 168: akapit górny: *„...przybliżone zostały w części 4. Rozdziału"*, akapit środkowy: *„Zgodnie z tym co zostało powiedziane w rozdziale III pracy"* i na dole: *„...przybliżone zostanie w części 4 rozdziału"*. Czasami Autor komplikuje niepotrzebnie tzw. akapity otwarcia starając się zdefiniować zakres danej części rozprawy, np.: *„Niniejszy rozdział pracy, otwierający część procesową całego opracowania poświęcony został próbie zbudowania definicji pojęcia „dowodu elektronicznego"..."* zamiast: „Niniejszy rozdział jest próbą zdefiniowania dowodu elektronicznego".

Autor w obszernej rozprawie decyduje się wielokrotnie na używanie zdań bardzo złożonych. Radzi sobie z tym dobrze. Jednakże czasami zapożycza konstrukcje z publicystyki albo nie panuje nad złożoną formą przekazu, np.: *„...przechodząc do ujęcia historycznego należy zaznaczyć, że kształtowanie się regulacji karnych cyberprzestrzeni jest procesem nadal aktualnym, toczącym się cały czas na naszych oczach"* (s. 26) (powinno być zresztą: regulacji karnych dla/wobec cyberprzestrzeni); *„Swoistym bohaterem pracy stała się cyberprzestrzeń"* (s. 6); *„Wszechobecny rozwój technologiczny, który stał się znakiem rozpoznawczym schyłku XX wieku"* (s. 21); *„...to jednak dopiero lata 80 stały się świadkiem jednych z najgłośniejszych w historii włamań komputerowych..."* (s. 27); *„...obowiązujących na ich terenie kodeksów karnych"* (s.30); *„...realizując zakreślone powyżej cele rozdziału, niniejsza część pracy porusza kolejno następujące zagadnienia"* (s. 293); *„Niemniej, ponieważ zapis danych pozostaje nierozerwalnie złączony z określonym nośnikiem..."* (s.307); *„...niniejszy rozdział stanowi zatem swoisty punkt zborny dla tematyki całej pracy..."* (s. 332); *„...nie jest możliwe*

mówienie w tym miejscu o stosowaniu prostej analogii" (s. 352); *„W doktrynie krajowej podkreśla się w szczególności, że mianem dowodu elektronicznego powinno określać się..."* (s. 294); *„Istotną bolączką obowiązujących w zakresie dowodów elektronicznych przepisów jest..."* (s.342).

Wiele zdań wymaga zmian bowiem tworzy konstrukcje nielogiczne, np. *„Powyższa problematyka zwracająca uwagę na aspekty okołoprawne ma istotne znaczenie..."* (s. 26); *„Należy zauważyć, że podział ten mając charakter czysto porządkowy, został zaproponowany jedynie by zapewnić czytelny sposób wprowadzenia poruszanej materii"* (s.127); *„W efekcie przyjętej budowy, oprócz zagadnień definicyjnych dotyczących cyberprzestępczości..."* (s. 163); *„...dla ukonstytuowania tak stypizowanego przestępstwa nie jest zatem istotne, czy zaatakowane dane mają jakiekolwiek znaczenie..."* (s.193); *„Jako przykłady negatywnych konsekwencji takiego stanu wskazać można na: (...) – problematykę dalszego wykorzystywania przez ofiarę ataku komputerów..."* (problematyka nie może być konsekwencją; tym bardziej, że pozostałe elementy enumeratywnej listy mają inną konstrukcję logiczną (ss. 342-343); *„Co stanowiło przedmiot wcześniejszych szczegółowych rozważań, podstawowym pojęciem stosowanym na gruncie prawa krajowego na określenie szeroko rozumianych elementów cyberprzestrzeni jest zwrot „system teleinformatyczny"*(s. 377).

Są też w rozprawie zdania, które poprzez swoją wadliwą konstrukcję pozwalają stawiać Autorowi zarzuty o co najmniej kontrowersyjne poglądy, np. *„Wciąż mała, choć powoli rosnąca, liczba opracowań w tym zakresie jest niewystarczająca by stawić czoło nie tylko obecnym, ale tym bardziej nadchodzącym wyzwaniom"* (s. 5); *„Z uwagi na interdyscyplinarny zakres pracy łączącej w sobie rozważania o charakterze stricte prawnym z elementami podstawowej wiedzy informatycznej, ale także dominację języka angielskiego w zakresie tematyki cyberprzestępczości w pracy pojawia się wiele terminów natury technicznej, w tym obcojęzycznych, których wprowadzenie jest jednak niezbędne dla wykorzystania w możliwie najpełniejszym zakresie aktualnego dorobku naukowego, tak prawnego jak i informatycznego w zakresie problematyki zwalczania cyberprzestępczości"* (s. 8 –

podkreślenia recenzenta); *„jako wniosek należy w tym zakresie podnieść zasadność uporządkowania odnośnych przepisów pod kątem stosowanej w nich siatki pojęciowej, tak by każda z ustaw branżowych posługiwała się jednolitym, wspólnym aparatem pojęciowym – a w konsekwencji także interpretacyjnym"* (s. 410).

9. Autor dokonał wnikliwej korekty ale nie ustrzegł się błędów w warstwie interpunkcyjnej czy fleksyjnej oraz tzw. literówek. Zatem dla porządku podaję zauważone: *„...ochrony wybranych kategorii informacji kluczowych do bezpieczeństwa państwa"* (powinno być: dla bezpieczeństwa państwa – s. 19); *„...nie tylko na przedstawienie szerokiej analiz zjawiska, ale..."* (powinno być: szerokiej analizy, s.8); *„...możliwość ustawicznego rozbudowywanie..."* (powinno być: ustawicznego rozbudowywania, s.119); *„...zgodnie z przepisami ustawy z dnia 5 sierpnia 2010 r. o ochronie niejawnych"* (powinno być: o ochronie informacji niejawnych, s. 192); *„...inicjującego postępowanie „z urzędu"* (powinno być: z urzędu, s. 192); *„...to jest kary 3 lat pozbawienie wolności"* (powinno być: pozbawienia wolności, s. 209); *„...osoby pobierające narzędzia oraz następnie wykorzystujące je zgodnie z udzieloną instrukcją, stają współsprawcami ataku"* (powinno być: stają się współsprawcami ataku, s. 230); *„Przesłanka te..."* (powinno być: Przesłanka ta, s.240); *„...zgodnie z przyjętą redakcją przepisu karne jest zatem nie tylko..."* (powinno być: przepisu karnego, s. 237); *„Bezwątpienia jeden z podstawowych atrybutów"* (powinno być: Bez wątpienia, s. 364); *„Kodeksowej definicji „przetwarzania danych"* (powinno być: kodeksowej definicji, s. 193); *„...oraz zawarte w niej informację..."* (powinno być: informacje, 336).

Błędy interpunkcyjne pojawiają się głównie przy określeniu *„w szczególności"* oraz *„także"* (np. s. 225) albo jako zbyt częste stosowanie przecinka. Autor sporadycznie nie panuje też nad redakcją tekstu, kiedy stosuje wyliczenia. Dla przykładu, kiedy opisuje implikacje wprowadzenia przesłanki przestępstwa zakłócenia pracy systemu komputerowego w art. 269a k.k., to przedstawia je w wyliczeniu kontynuowanym. Podobnie utrudnia lekturę wyliczenie na stronach 232-233.

III. Ocena warstwy metodologicznej rozprawy

1. Lektura rozprawy doktorskiej mgr. Janusza Konrada Wasilewskiego daje podstawy do stwierdzenia, że proces badawczy, jaki Autor przeprowadził jest prawidłowy. Przedmiotem badań prowadzonych w rozprawie jest problematyka fluktuacji prawa karnego materialnego definiującego cyberprzestępstwa oraz prawnych aspektów ich zwalczania. Autor zastrzega (s. 10), że badania nie mają jedynie charakteru dogmatycznego. Lektura rozprawy potwierdza to założenie. Zastosowano w badaniach metodę: dogmatyczną, komparatystyczną, analizy piśmiennictwa i badania dokumentów. Praca ma niewątpliwie charakter interdyscyplinarny. Autor łączy rozważania prawne z technicznymi. Takie podejście jest możliwe dzięki zarówno wysokiej dojrzałości prawniczej i intelektualnej Doktoranta, jak i Jego szerokim zainteresowaniom profesjonalnym w dziedzinie informatyki.

2. Na wysoką ocenę zasługuje sposób prowadzenia rozważań komparatystycznych. Autor sięga do aktów prawa międzynarodowego (najczęściej do Konwencji Rady Europy o cyberprzestępczości) i prawa unijnego (np. Decyzja Ramowa rady Unii Europejskiej z 24.02.2005 w sprawie ataków na systemy informatyczne) oraz prawa krajowego – polskiego i wybranych innych państw (interesująca tablica porównawcza rozwiązań prawnych znajduje się na ss. 121-123) ale także rozwiązań poza karnych. Schemat porównawczy stosuje konsekwentnie przede wszystkim w rozdziałach III i IV. Pewne jego elementy wykorzystywane są też w rozdziale VI. Autor stosuje tu zresztą rzadko występujący podział badawczy – ujęcie statyczne (opis zagrożenia – domena prawa karnego materialnego) i ujęcie dynamiczne (problematyka zwalczania). Twierdzi się, we wstępie, że badania autorskie miały także charakter empiryczny. Faktycznie Autor stara się prezentować często i szeroko przykładowe mechanizmy popełniania przestępstw i daje tym

samym istotne wsparcie dla komentarza w płaszczyźnie statycznej. Rzadziej czyni to w płaszczyźnie dynamicznej (stosując Jego nomenklaturę badawczą).

3. Szeroki zakres badań zdecydował o przyjęciu przez Autora specyficznej metody wyznaczenia ogólnych celów badawczych – w podziale na odcinki badawcze. Wyznacza się sześć takich odcinków: analizę stanu prawnego w zakresie legalnego definiowania cyberprzestrzeni, przybliżenie (?) wybranych aspektów technicznych budowy oraz funkcjonowania sieci komputerowych, analizę stanu prawnego w zakresie legalnego definiowania cyberprzestępczości, analizę możliwości przyjęcia nowego podziału cyberprzestępczości, analizę cyberprzestępstw o najwyższej doniosłości pragmatycznej prowadzoną w ujęciu zarówno prawnym, jak i merytorycznym oraz ocenę obowiązujących przepisów krajowych pod kątem ich zastosowania do zwalczania cyberprzestępczości (ss. 9-10). W ich ramach skonstruowane zostały precyzyjnie ogólne i szczegółowe pytania badawcze. Ogólne hipotezy badawcze są następujące: a) stan prawny w zakresie legalnego definiowania cyberprzestrzeni posiada istotne braki normatywne; b) zrozumienie kwestii prawnych dotyczących szeroko rozumianej regulacji cyberprzestrzeni pozostaje bezpośrednio uwarunkowane procesem poznania podstawowych aspektów technicznych z zakresu budowy oraz funkcjonowania tego obszaru na poziomie infrastrukturalnym oraz sprzętowo-programowym; c) stan prawny w płaszczyźnie krajowej i międzynarodowej w zakresie legalnego definiowania cyberprzestępczości zawiera istotne luki legislacyjne; d) powszechnie stosowana typologia cyberprzestępczości z zastosowaniem kryterium naruszanego dobra prawnie chronionego nie jest właściwa dla opisu zjawiska cyberprzestępczości; e) w obowiązującym stanie prawnym poszczególne typy cyberprzestępstw ujmowane są w sposób niespójny i nie kompleksowy, bez wyraźnego rozdziału poszczególnych przestępstw; f) obowiązujące w kraju regulacje karno-procesowe nie identyfikują oraz nie ujmują w sposób należyty specyfiki zwalczania cyberprzestępczości (ss. 14 – 17).

Uważam, że cele badań i hipotezy główne są tak skonstruowane, że świadczą o wysokiej jakości rozprawy.

4. Tezą rozprawy mgr. Janusza Wasilewskiego jest założenie prawne, iż specyfika techniczna cyberprzestrzeni zmodyfikowała sposób pojmowania typowych instytucji prawnych w stopniu tak istotnym, iż wymagają one nowego podejścia interpretacyjnego lub wręcz zasadniczego przeformułowania ich konstrukcji prawnych (s. 405). Autor potrafi te rozważania zakończyć dojrzałymi wnioskami, które prezentuje w trzech płaszczyznach. Po pierwsze, twierdzi, że w przypadku cyberprzestrzeni mamy do czynienia z jednoznacznym ukształtowaniem się nowej domeny ludzkiej aktywności, posiadającej nieznaną wcześniej cechę „wirtualności" zaś pozbawioną znanych cech fizycznych, jak wymiary, odległości czy topografia geograficzna (s. 406). Po drugie, Autor formułuje szereg wniosków i postulatów w zakresie regulacji zjawiska cyberprzestępczości. Po trzecie, wskazuje na konieczność zmian w sposobie pojmowania czynności procesowych realizowanych w domenie cyfrowej. Sposób i jakość formułowania wniosków zasługuje na bardzo wysoką ocenę.

IV. Merytoryczna ocena rozprawy

1. Recenzowana praca stanowi dzieło bardzo interesujące i wartościowe. Może być inspiracją dla poszukiwania nowych kierunków badawczych. Zasługuje na pozytywną ocenę. W warstwie szczegółowej pragnę sformułować kilka uwag merytorycznych, istotnych dla uzasadnienia tej oceny ale też wyznaczających kierunki dalszych badań mgr. Janusza Wasilewskiego. Cyberprzestrzeń bowiem rozwijać będzie się dalej bardzo dynamicznie i stanowić będzie obszar ciągłej penetracji przestępców. Trudno zgodzić się jednakże z Autorem, że problematyka cyberprzestępczości stanowi *novum*. Tak nie jest. Ważne jest natomiast, aby badacze

decydowali się proponować metodykę bardziej opartą na empirii, byli jeszcze bardziej dociekliwi w obszarze opisu *modus operandi* oraz zdeterminowani w proponowaniu nowych rozwiązań prudencyjnych czy karnoprawnych. Autor sam wskazuje, że rozważania prawnicze najczęściej opierają się wyłącznie na analizie dogmatycznej, nie wnikając w stronę merytoryczną zjawiska (s. 9). Trudno nie zgodzić się z tym stanowiskiem. Autor sam próbuje wyznaczać kierunki dalszego badania naukowego. Jego praca, co raz jeszcze podkreślam, świadczy o wysokim potencjale i życzyć należy Panu magistrowi sukcesów na polu wnikania w merytoryczną stronę cyberprzestępczości, co służyć może w konsekwencji podnoszeniu poziomu bezpieczeństwa państwa.

2. Na początek egzemplifikować należy pogląd, który Autor prezentuje w kilku miejscach rozprawy. Otóż twierdzi, że to cyberataki, ataki terrorystyczne czy inne kategorie działań przestępczych dają asumpt do tworzenia nowych rozwiązań karnoprawnych oraz przepisów dających możliwość skuteczniejszych działań organów ścigania (podaje przykład ataków terrorystycznych na World Trade Center oraz rozwiązań amerykańskiej Patriot Act – s. 33). Całkowicie utożsamiam się z tym poglądem i wspieram Autora w propagowaniu takiego podejścia w ramach uprawianej dyscypliny.

3. Uznaję nowatorstwo zaproponowanej klasyfikacji cyberprzestępstw a także traktuję ją jako wartość dodaną w tym obszarze badawczym. Uważam, że kryterium budowy cyberprzestrzeni oraz transmisji danych pozwala na prezentowaną przez Autora klasyfikację i ułatwia merytoryczną dyskusję na temat praktycznych aspektów zwalczania tego zagrożenia.

4. Komentarz prawniczy, który proponuje Autor jest w niektórych miejscach pasjonujący. Stawiane są pytania szczegółowe co do określonych stanów faktycznych. Jednocześnie wskazuje się obszary, w których określone zachowania

niepożądane w cyberprzestrzeni nie podlegają penalizacji albo co najmniej może być trudne ich interpretowanie przy wykorzystaniu aktualnie obowiązujących przepisów. Dla przykładu, należy zgodzić się z Autorem, że brak desygnatu pojęcia „informacja", przekreśla możliwość wystąpienia ustawowej przesłanki „dostępu do informacji", czy też „uzyskania informacji" wykluczając tym samym byt samego przestępstwa uregulowanego w art. 267 § 1 oraz § 3 kodeksu karnego (s. 178). Jednocześnie Autor potrafi wiele tego typu problemów interpretować i prezentować tradycyjne podejście prawne oparte na zbiegu przestępstw (np. bezprawnego podsłuchu i nieuprawnionej modyfikacji treści transmisji – s. 186). W sukurs w tym zakresie nie zawsze przychodzi analiza prawnoporównawcza. Autor posługuje się tu wykładnią językową, w szczególności przy wykorzystaniu tłumaczeń z języka angielskiego. W tym zakresie naturalnie poszukuje rozszerzeń znaczeniowych (jako przykład należy podać tu intersujący komentarz Autora dotyczący przestępstwa nieuprawnionego modyfikowania lub uszkadzania danych transmitowanych za pośrednictwem sieci i wykorzystania w nim znaczenia odpowiedniego przestępstwa na gruncie Konwencji Rady Europu o cyberprzestępczości – *suppresion*) (s. 190).

Stosuje też wykładnię systemową. W tym kontekście można jednak polemizować z Autorem co do poprawności Jego wywodów, np. w komentarzu do art. 268a k.k. i 289 k.k. podważa logikę stosowania definicji z ustawy o danych osobowych oraz ustawy o ochronie informacji niejawnych do pojęcia „przetwarzanie danych" (s.193).

5. Autor dokonuje wielokrotnie podziału cyberprzestępstw w kontekście kategorii danych czy informacji (państwowe – prywatne). Podział ów jest jak najbardziej zasadny (nawet zakładając, że państwowe dane są zbiorem węższym niż dane publiczne). Nie wiadomo jednakże, dlaczego stosuje wobec tej kategorii cudzysłów. Wydaje się, że kategoria danych publicznych w szczególności chroniona powinna być karnoprawnie i do niej w najbliższych latach kierowane będą różne

rozwiązania, o których traktuje m.in. rozdział VI rozprawy Pana Janusza Wasilewskiego.

6. W rozprawie wielokrotnie podkreśla się, że systemy komputerowe rozwijają się najdynamiczniej spośród wszystkich przejawów cywilizacji. W tym kontekście swoiste ograniczenie znajduję w podejściu Autora do komentarza normy art. 269a k.k. Twierdzi On, że poza zakresem „sieci teleinformatycznej" czy systemu komputerowego pozostają urządzenia takie, jak nowoczesne smartfony czy tablety z modemem 3G, będące w istocie hybrydami urządzeń komputerowych oraz telefonów komórkowych, a także wysoce specjalistyczne systemy produkcyjne (np. roboty w fabryce samochodów) i wreszcie systemy SCADA (s. 212). Takie ujęcie wyraźnie kłóci się ze stosowanym wielokrotnie w rozprawie. To podkreślenie jest dla mnie tym bardziej nie do przyjęcia z jeszcze innego powodu. Otóż Autor opisując system SCADA wskazuje, że obsługuje on m.in. elektrownie atomowe, przepompownie wody, tamy. Zupełnie niepotrzebnie daje przykłady, które w Polsce występują rzadko albo wcale a nie wskazuje zastosowań, które są powszechne i dodatkowo często narażone na zakłócenia, tak techniczne, jak i przestępcze. Mam tu na myśli obszar dystrybucji energii elektrycznej. W tym zakresie zresztą znajduję istotny błąd interpretacyjny w komentarzu Autora do art. 269a k.k. (ss. 212-213). Twierdzi On, że nietrafne jest użycie w przepisie określenia „praca systemu komputerowego lub sieci teleinformacyjnej" a właściwsze jest: „automatyczne przetwarzanie danych". Wydaje się natomiast, że w kontekście systemów takich jak SCADA zdecydowanie pojemniejszy termin „praca systemu komputerowego" wyczerpuje pełniej znaczenie czynów definiowanych w art. 269a k.k.

7. W rozprawie znaleźć można cały szereg uwag krytycznych wobec cyberprzestępstw stypizowanych w kodeksie karnym. W precyzyjny sposób Autor komentuje mankamenty polskiego prawa wskazując, jakie stany faktyczne nie wyczerpują znamion określonych w przepisach przestępstw. Jako przykład można

podać instytucję przesłanki uzyskania dostępu do treści pornograficznych z udziałem małoletniego wymienionej *expressis verbis* w przepisie art. 202 § 4a k.k. Przesłanka ta, wymagając z jednej strony przeprowadzenia trudnego dowodowo potwierdzenia, iż sprawca określonego czynu rzeczywiście uzyskał faktyczny dostęp do materiału prawnie zabronionego (co wydaje się wykraczać poza zwykłe stwierdzenie, iż sprawca „pobrał" z sieci dany materiał), z drugiej strony – z uwagi na swój obiektywny charakter, może stać się podstawą do oskarżenia o popełnienie definiowanego w tym przepisie czynu osoby, która nawet nie tyle została wprowadzona w błąd, w efekcie którego pozyskała dany plik (np. poprzez nakłonienie do kliknięcia mylnie oznaczonego odsyłacza internetowego), co wręcz osoby, której np. umyślnie wysłano na jej skrzynkę poczty internetowej materiały zawierające zabronione prawem treści pornograficzne (s. 240).

8. W części procesowej rozprawy zdecydowanie bardziej interesujące są rozważania merytoryczne dotyczące transpozycji czynności procesowych do obszaru cyberprzestrzeni (rozdział VI) niż te, w których charakteryzuje się dowód elektroniczny (rozdział V). Autor w rozdziale V decyduje się na bardzo skomplikowane i szerokie porównania semantyczne i analizę prawnoporównawczą na gruncie prawa polskiego i międzynarodowego różnych terminów, które wiążą się w jakikolwiek sposób z dowodem elektronicznym – informacja, dane, dane komputerowe. Tymczasem ostatecznie w tej części najważniejsze pozostaje zdefiniowanie dowodu elektronicznego poprzez jego szczególną formę wyrażającą się w elektronicznym zapisie, nie pozwalającym na odczyt treści materiału bez zastosowania stosownego urządzenia do przetwarzania informacji (s. 330). Istotne pozostają też wszystkie kwestie tego rozdziału, które mają znaczenie dla rozważań w ostatnim rozdziale – a to przede wszystkim: rodzaje urządzeń i nośników dowodu elektronicznego, typy dowodów elektronicznych oraz przykładowe ujęcia poczty e-mailowej jako źródła dla pozyskiwania dowodów elektronicznych.

9. Autor podnosi w ostatnim rozdziale kwestie merytoryczne zasadnicze dla skutecznego zwalczania cyberprzestępczości. Brak wyraźnego rozdzielenia prawnego pomiędzy nośnikiem a samym dowodem powoduje w konsekwencji konieczność traktowania, jako dowodów głównie fizycznych nośników, dających się opisać, zaewidencjonować oraz dołączyć do prowadzonych wciąż w postaci papierowej akt sprawy (s. 342). Kwestie skuteczności zwalczania Autor stawia właściwie w kontekście zapewnienia zgodności działań wykrywczych z Konstytucją Rzeczypospolitej Polskiej oraz z prawami obywatelskimi. Za niedopuszczalne uznaje wszelkie próby automatycznego, domyślnego przypisywania winy za atak właścicielowi (dzierżawcy) danego łącza, z którego atak ten został wyprowadzony (winy nie ponosi przecież łącze, ani komputer, zaś wobec osób funkcjonuje konstytucyjnie sankcjonowane domniemanie niewinności). Ustalenie miejsca stanowi bowiem wyłącznie punkt wyjściowy do prowadzenia dalszych poszukiwań narzędzia zbrodni, jakim w tym wypadku jest określony system teleinformatyczny (s. 348).

10. Autor profesjonalnie porządkuje wątki w coraz szerszej dyskusji na temat prowadzenia czynności procesowych za pośrednictwem cyberprzestrzeni. Zgodzić trzeba się z Nim, że rozwój w tym zakresie determinowany jest zarówno przez nowe rozwiązania prawne, jak i konieczne tworzenie infrastruktury w samych organach ścigania realizujących te czynności. Do determinantów tych zalicza np. istotne ułatwienia w faktycznym realizowaniu uprawnień procesowych przez organy ścigania czy możliwość szerokiego stosowania dowodów elektronicznych zdobywanych w ramach prostego zabezpieczenia dokonywanego przez odpowiednio przeszkolonego funkcjonariusza (s. 356). W tym kontekście niezwykle ważkie są rozważania Autora na temat zdalnego przeszukania. Otóż na gruncie kodeksu postępowania karnego czynność ta nie znajduje żadnego oparcia, ale stanowi wręcz naruszenie szeregu zasad procesowych, jak choćby gwarancji udziału osób objętych przeszukaniem w prowadzonej czynności. Co więcej – żadna z tzw. ustaw policyjnych, jak również sam kodeks karny, nie przewidują w obecnym brzmieniu

stosownych uprawnień oraz skorelowanych z nimi kontratypów, które dopuszczałyby podejmowanie przez służby krajowe czynności zdalnego przeszukania dowolnych zasobów cyberprzestrzeni (s. 390).

V. Konkluzja

1. Stwierdzam jednoznacznie, że rozprawa doktorska mgr. Janusza Konrada Wasilewskiego pt. *Cyberprzestępczość – wybrane aspekty prawnokarne oraz kryminologiczne* spełnia kryteria określone w art. 13 ust. 2 ustawy z dnia 14 marca 2004 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (Dz.U z 2014 r., poz. 1852 z późn. zm.) i stanowi oryginalne rozwiązanie problemu naukowego a także potwierdza głęboką wiedzę teoretyczną Kandydata w zakresie nauk prawnych.

2. Wnoszę o dopuszczenie Pana mgr. Janusza Konrada Wasilewskiego do dalszych etapów postępowania w przewodzie doktorskim.