Lublin dnia 20 października 2025 r.

prof. ucz. dr hab. nauk prawnych Grzegorz Tylec
Katolicki Uniwersytet Lubelski Jana Pawła II
Instytut Dziennikarstwa i Zarządzania
Kierownik Katedry Języka, Retoryki i Prawa Mediów

Recenzja
osiągnięć naukowych dr Marka Porzeżyńskiego
sporządzona w postępowaniu o nadanie stopnia doktora habilitowanego

Postępowanie habilitacyjne. Podstawa prawna

Zgodnie z art. 219 ust. 1 ustawy z dnia 11 marca 2022 r. Prawo o szkolnictwie wyższym (Dz.U.2024.1571 t.j.) stopień doktora habilitowanego nadaje się osobie, która:

1) posiada stopień doktora;

2) posiada w dorobku osiągnięcia naukowe albo artystyczne, stanowiące znaczny wkład w rozwój określonej dyscypliny, w tym co najmniej:

a) 1 monografię naukową wydaną przez wydawnictwo, które w roku opublikowania monografii w ostatecznej formie było ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. a, lub

b) 1 cykl powiązanych tematycznie artykułów naukowych opublikowanych w czasopismach naukowych lub w recenzowanych materiałach z konferencji międzynarodowych, które w roku opublikowania artykułu w ostatecznej formie były ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. b, lub

c) 1 zrealizowane oryginalne osiągnięcie projektowe, konstrukcyjne, technologiczne lub artystyczne;

3) wykazuje się istotną aktywnością naukową albo artystyczną realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.

Sylwetka Habilitanta i ogólna charakterystyka jego dorobku naukowego

Dr Marek Porzeżyński jest prawnikiem i badaczem specjalizującym się w zagadnieniach prawa nowych technologii, cyberbezpieczeństwa, danych osobowych oraz ochrony własności intelektualnej, ze szczególnym uwzględnieniem ochrony programów komputerowych i zastosowań sztucznej inteligencji w praktyce prawniczej. Swoją ścieżkę akademicką rozpoczął na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego, gdzie w 2013 r. uzyskał tytuł magistra prawa na podstawie pracy magisterskiej pt. „Cywilnoprawne metody ochrony domen internetowych" napisanej pod kierunkiem prof. dr hab. Wojciecha Kocota. Jeszcze w trakcie studiów w 2012 r., ukończył studia podyplomowe z zakresu prawa własności intelektualnej organizowane przez Centrum Praw Własności Intelektualnej im. H. Grocjusza w Krakowie. W 2016 r. uzyskał stopień naukowy doktora nauk prawnych w zakresie prawa na podstawie uchwały Rady Wydziału Prawa Uniwersytetu SWPS w Warszawie. Rozprawę doktorską pt. „Zdolność patentowa programów komputerowych" przygotował pod opieką prof. dr hab. Jacka Sobczaka, a recenzentkami w przewodzie były prof. dr hab. Krystyna Szczepanowska-Kozłowska i prof. dr hab. Joanna Sieńczyło-Chlabicz. W 2019 r. ukończył anglojęzyczny program studiów MBA – Innovation and Data Analysis, zorganizowany przez Instytut Podstaw Informatyki Polskiej Akademii Nauk (IPI PAN) we współpracy z Woodbury School of Business (akredytacja AACSB) oraz Utah Valley University. Obronił projekt dyplomowy pt. „Utilization of Artificial Intelligence in Legal Industry" pod kierunkiem Serge'a Pukasa. W kolejnych latach doskonalił swoje kompetencje na styku prawa, informatyki i zarządzania bezpieczeństwem informacji, uzyskując szereg certyfikatów międzynarodowych. Równolegle podejmował studia inżynierskie na kierunku informatyka stosowana na Wydziale Elektrycznym Politechniki Warszawskiej (zrealizowane przedmioty z drugiego i trzeciego roku), które przerwał w 2020r. w związku z rozpoczęciem pracy naukowo-dydaktycznej na tej uczelni. Habilitant karierę akademicką rozpoczął w 2013 r. jako asystent w Katedrze Prawa Informatycznego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego, gdzie prowadził zajęcia z prawa własności intelektualnej, prawa nowych technologii i cyberbezpieczeństwa. W latach 2016–2020 był wykładowcą na Wydziale Prawa Uniwersytetu SWPS w Warszawie, gdzie prowadził zajęcia z ochrony własności intelektualnej, prawa nowych technologii i cyberbezpieczeństwa. Od 2018 r. współpracuje z Uczelnią Łazarskiego w Warszawie jako wykładowca w ramach studiów podyplomowych „Prawo w biznesie nowych technologii", prowadząc zajęcia z ochrony programów komputerowych. Od 2021 r. związany jest z Politechniką Warszawską, Wydziałem

Administracji i Nauk Społecznych, Zakład Prawa Administracyjnego i Nauki o Politykach Publicznych, gdzie pełni funkcję adiunkta, a od 2024 r. również Prodziekana ds. Studenckich.

Dorobek naukowy i dydaktyczny dr Marka Porzeżyńskiego łączy perspektywę prawniczą i technologiczną, jego prace koncentrują się na przecięciu prawa i informatyki, a doświadczenie w obszarze audytu bezpieczeństwa informacji i standardów ISO 27001 znajduje zastosowanie w badaniach dotyczących zgodności systemów informatycznych z wymogami prawa.

Ocena rozprawy habilitacyjnej

Wybór i sformułowanie tematu pracy

Jako rozprawę habilitacyjną Habilitant przedstawił monografię pt „Cyberbezpieczeństwo dostawców usług cyfrowych", Warszawa 2021, wydaną przez Instytut Wydawniczy EuroPrawo Sp. z o.o., ISBN: 978-83-7627-209-2 (275 s.). Tytuł książki habilitacyjnej został dobrany prawidłowo, jest on aktualny zarówno z punktu widzenia naukowego, jak i praktycznego. Autor trafnie identyfikuje zjawisko, które w ostatnich latach zyskało na znaczeniu w wyniku rozwoju gospodarki cyfrowej, wzrostu liczby incydentów cyberbezpieczeństwa oraz implementacji unijnych regulacji w postaci Dyrektywy NIS i krajowej ustawy o krajowym systemie cyberbezpieczeństwa. Wybór problematyki cyberbezpieczeństwa dostawców usług cyfrowych należy uznać za oryginalny i potrzebny w polskim piśmiennictwie prawniczym. O ile temat cyberbezpieczeństwa był już przedmiotem licznych opracowań ogólnych, o tyle szczegółowe ujęcie dotyczące wąskiej, ale niezwykle istotnej kategorii podmiotów – dostawców usług cyfrowych stanowi lukę badawczą, którą Autor w sposób świadomy i konsekwentny podejmuje. Sformułowanie tematu pracy wskazuje na jasno określony zakres przedmiotowy i podmiotowy pracy. Autor nie ogranicza się do omówienia norm prawnych, lecz analizuje także instytucjonalny, organizacyjny i techniczny wymiar cyberbezpieczeństwa, co pozwala na interdyscyplinarne ujęcie zagadnienia. Tytuł książki jest adekwatny do jej treści i oddaje istotę rozważań, łącząc aspekt prawnonormatywny (obowiązki i odpowiedzialność dostawców) z kontekstem praktycznym (wdrażanie systemów bezpieczeństwa, relacja z organami nadzoru, wykorzystanie standardów ISO i ENISA). Na uznanie zasługuje również sposób sformułowania tematu, który jest konkretny, komunikatywny i precyzyjny. Autor unika zbyt szerokich lub ogólnych określeń koncentrując się na jasno zdefiniowanym segmencie rynku usług cyfrowych i jego regulacji. Dzięki temu książka ma wyraźnie zarysowany profil badawczy i praktyczną przydatność.

Jedynym ograniczeniem w zakresie doboru tematu może być wąski kontekst sektorowy, skupienie się niemal wyłącznie na dostawcach usług cyfrowych, bez szerszej analizy ich relacji z operatorami usług kluczowych czy administracją publiczną. Jednak z metodologicznego punktu widzenia takie zawężenie jest uzasadnione i sprzyja pogłębionej analizie problemu. Podsumowując, temat książki został wybrany trafnie a jej tytuł jest precyzyjny. Autor podjął się opracowania problemu ważnego społecznie i gospodarczo, a przy tym wciąż niedostatecznie opracowanego w polskiej literaturze prawniczej.

Nowość osiągnięcia naukowego i jego wkład w rozwój dyscypliny naukowej

Analiza dorobku naukowego Habilitanta wskazuje, że w jego dotychczasowym dorobku naukowym znajdują się tylko trzy opracowania naukowe, które jedynie pośrednio dotyczą zagadnienia objętego zakresem monografii habilitacyjnej. Są to: M. Porzeżyński, Ł. Kulicki, *Changes introduced by the NIS Directive 2.0 and their potential effects on the cybersecurity labour market*, Cybersecurity and Law vol. 11, 2024.; M. Porzeżyński, *Problematyka rozprzestrzeniania nieprawdziwych informacji jako zagadnienia społecznego i prawnego*, Horyzonty Bezpieczeństwa 2018, nr 11; M. Porzeżyński, *Zarządzanie bezpieczeństwem informacji w świetle wymagań cyberbezpieczeństwa w Polsce,* w: M Porzeżyński, A Borcuch (red.), *Bezpieczeństwo w erze społeczeństwa informacyjnego. Dylematy i wyzwania*, Laboratorium Wiedzy Artur Borcuch, Kielce 2019. Zestawiając wskazane powyżej teksty z monografią habilitacyjną stwierdzić należy, że nie są one w monografii nawet w części powtórzone. Mając na uwadze przedstawione we wstępie rozprawy habiltacyjnej tezy badawcze oraz szczegółowe pytania badawcze oraz zawarte na łamach pracy wywody, monografię habilitacyjną uznać należy za zakresowo odmienną w stosunku do pozostałego dorobku naukowego Habilitanta oraz za osiągnięcie stanowiące znaczący wkład w rozwój dyscypliny naukowej.

Cele badawcze i metodologia rozprawy habiltacyjnej

Recenzowana rozprawa została zaprojektowana jako opracowanie naukowe o wyraźnie analityczno-dogmatycznym charakterze, którego celem jest zrekonstruowanie i ocena obowiązującego systemu prawnego w zakresie cyberbezpieczeństwa dostawców usług cyfrowych, a także określenie ich roli w krajowym i europejskim systemie bezpieczeństwa cyfrowego.

Autor precyzyjnie określa główne i szczegółowe cele pracy. Głównym celem badawczym jest: „ustalenie zakresu obowiązków oraz odpowiedzialności dostawców usług cyfrowych w świetle Dyrektywy NIS oraz ustawy o krajowym systemie cyberbezpieczeństwa, a także ocena skuteczności przyjętych rozwiązań prawnych w kontekście ochrony infrastruktury cyfrowej". Cele szczegółowe obejmują w szczególności: analizę genezy i ewolucji regulacji unijnych w obszarze cyberbezpieczeństwa, zdefiniowanie pojęcia i statusu prawnego dostawców usług cyfrowych, omówienie obowiązków nałożonych na dostawców usług cyfrowych w ramach krajowego systemu cyberbezpieczeństwa, identyfikację problemów interpretacyjnych i praktycznych wynikających z implementacji Dyrektywy NIS, odniesienie rozwiązań polskich do regulacji w innych państwach członkowskich (analiza porównawcza), przedstawienie relacji pomiędzy regulacjami prawnymi a standardami technicznymi (np. ISO/IEC, ENISA). Cele te zostały sformułowane klarownie i konsekwentnie rozwijane w kolejnych rozdziałach. Autor zachował spójność pomiędzy założeniami badawczymi a strukturą pracy, kolejne rozdziały odpowiadają logicznie poszczególnym etapom realizacji celu głównego (od kontekstu teoretycznego i normatywnego po analizę implementacyjną i praktyczną).

W warstwie metodologicznej Autor posługuje się przede wszystkim metodą dogmatyczno-prawną, polegającą na analizie obowiązujących aktów prawnych, ich wykładni systemowej, językowej i celowościowej, oraz badaniu relacji między przepisami prawa krajowego i unijnego. W pracy zastosowano również metodę analizy porównawczej (porównanie rozwiązań w Polsce, Niemczech, Francji, Wielkiej Brytanii) oraz metodę systemową, pozwalającą ująć problem cyberbezpieczeństwa w szerszym kontekście relacji między regulacjami prawnymi, instytucjami i standardami technicznymi. Autor wprowadza ponadto elementy analizy interdyscyplinarnej, łącząc instrumenty prawa z perspektywą nauk technicznych i bezpieczeństwa informacji. Dobór metodologii należy uznać za trafny i adekwatny do charakteru tematu. Problem cyberbezpieczeństwa dostawców usług cyfrowych wymaga przede wszystkim precyzyjnej analizy przepisów prawa, dlatego dominacja metody dogmatyczno-prawnej była właściwym wyborem. Uzupełnienie jej o analizę komparatystyczną i odniesienia techniczne pozwoliło Autorowi zachować równowagę między teorią prawa a realiami stosowania norm w praktyce. Pewnym ograniczeniem metodycznym jest brak wyraźnego komponentu empirycznego (np. analizy orzecznictwa, praktyki stosowania przepisów lub badań jakościowych wśród dostawców usług cyfrowych). Jednak w świetle charakteru pracy, opartej głównie na analizie prawa, brak ten nie obniża wartości naukowej opracowania.

Ten aspekt pracy ocenić należy całkowicie pozytywnie. Na podkreślenie zasługuje rzetelność warsztatu badawczego oraz duża znajomość aspektów technologicznych badanych instytucji co świadczy o wartości naukowej prowadzonych rozważań oraz o wadze sformułowanych wniosków.

Konstrukcja pracy oraz jej strona warsztatowa

Rozprawa charakteryzuje się przemyślaną i logiczną konstrukcją, która odpowiada klasycznemu schematowi monografii naukowej o profilu prawniczym. Układ treści jest klarowny i hierarchiczny, od rozdziałów wprowadzających o charakterze definicyjno-teoretycznym (rozdz. I–II), przez część dogmatyczno-prawną (rozdz. III–IV), aż po fragmenty o wymiarze praktycznym i aplikacyjnym (rozdz. V). Każdy rozdział ma wyraźnie określony cel cząstkowy, który pozostaje w relacji do głównego celu badawczego. Autor konsekwentnie rozwija problematykę, unikając dygresji i zachowując spójność narracyjną. Przejścia między rozdziałami są płynne, a całość zamyka logiczne podsumowanie, które syntetyzuje ustalenia i wskazuje kierunki dalszych badań.

Autor wykazuje wysoki poziom kompetencji badawczej i bardzo dobre opanowanie warsztatu naukowego w zakresie prawa. Praca bazuje na szerokim korpusie źródeł, obejmującym: akty prawa unijnego, akty prawa krajowego, dokumenty instytucji międzynarodowych, piśmiennictwo naukowe polskie i zagraniczne, raporty branżowe i opracowania eksperckie. Autor korzysta zarówno z klasycznych pozycji doktryny prawa, jak i nowoczesnych opracowań z zakresu zarządzania bezpieczeństwem informacji i technologii cyfrowych. Cytowania są poprawne, a odniesienia bibliograficzne precyzyjne.

Język pracy jest klarowny, rzeczowy i precyzyjny, zgodny ze standardami wypowiedzi naukowej w dziedzinie nauk prawnych. Wywód prowadzony jest logicznie i konsekwentnie, zdarzają się fragmenty o dużym stopniu formalizmu (szczególnie przy omawianiu przepisów), jednak nie wpływa to negatywnie na przejrzystość tekstu. Praca jest wolna od błędów językowych, logicznych i redakcyjnych.

Recenzowana rozprawa prezentuje wysoki poziom warsztatowy, odpowiadający standardom publikacji naukowej w dyscyplinie nauk prawnych. Zastosowane metody badawcze, sposób prowadzenia wywodu oraz jakość języka i konstrukcji tekstu świadczą o pełnej dojrzałości naukowej autora.

Uwagi merytoryczne

Generalnie na akceptację zasługują konkluzje, do których Autor dochodzi w rozprawie. Generalna akceptacja tez pracy nie oznacza jednak, że wywody dotyczące poszczególnych kwestii w całości zasługują na akceptację lub nie wywołują różnorakich wątpliwości. Niektóre stwierdzenia przedstawione w rozprawie mają charakter dyskusyjny budzą wątpliwości lub niedosyt. Podkreślić należy, że wytknięte usterki mają głównie charakter dyskusyjny. Przede wszystkim uważam, że zgłoszone uwagi nie dotyczą zagadnień pierwszoplanowych a więc, w konsekwencji, nie mają zasadniczego znaczenia dla całościowej oceny pracy, która to ocena jest pozytywna. Ponieważ poniższe uwagi mają charakter szczegółowy przedstawiam je w kolejności wynikającej z toku wywodu recenzowanej rozprawy, niezależnie od znaczenia.

W rozdziale pierwszym Autor trafnie ukazuje cyberbezpieczeństwo jako dziedzinę na pograniczu prawa, nauk technicznych, informatyki i zarządzania. Odwołuje się do aktualnego stanu klasyfikacji dyscyplin naukowych w Polsce, wskazując, że problematyka ta jest obecna w naukach społecznych, technicznych i prawnych. Rozdział ten nie ogranicza się tylko do rozważań teoretycznych, w wielu miejscach wskazuje praktyczne odniesienia do polityk bezpieczeństwa, norm (np. ISO/IEC 27001), czy aktów prawnych, co wzmacnia użyteczność tych wprowadzających rozważań. Choć analizowana część pracy dobrze prezentuje terminologię, brakuje w niej wskazania celu poznawczego, nie jest jasne, czy Autor chce tylko uporządkować pojęcia, czy także je krytycznie ocenić lub zaproponować nowe ujęcie definicyjne. Rozdział ten przez to miejscami przypomina kompendium, a nie analizę naukową. Duża liczba cytatów i źródeł wprowadza bogactwo materiału, ale jednocześnie powoduje, że tekst traci spójność analityczną. Niektóre podrozdziały sprawiają wrażenie przeglądu literatury bez wyraźnego komentarza Autora. Podsumowując rozdział I pełni funkcję solidnego wprowadzenia, ale nie wnosi innowacyjnych elementów poznawczych.

W rozdziale II Autor w sposób bardzo systematyczny i obszerny przedstawia kluczowe dokumenty strategiczne, polityczne i prawne dotyczące cyberbezpieczeństwa zarówno na poziomie międzynarodowym (ONZ, NATO, Rada Europy, Unia Europejska), jak i krajowym (strategie rządowe RP, doktryna cyberbezpieczeństwa, programy ochrony cyberprzestrzeni). To przekrojowe ujęcie pozwala czytelnikowi dostrzec ewolucję podejścia do cyberbezpieczeństwa w ostatnich latach. W tej części pracy Autor samodzielnie analizuje teksty źródłowe, przytacza ich kontekst, cele i ograniczenia, a w wielu miejscach dodaje własne komentarze krytyczne co nadaje rozdziałowi charakter naukowej analizy źródłowej. Autor nie ogranicza się do prezentowania treści dokumentów, lecz ocenia ich realność, ogólność i skuteczność. Niestety jak zauważa sam Autor większość analizowanych

dokumentów nie odnosi się bezpośrednio do dostawców usług cyfrowych. Oznacza to, że rozdział ten mimo wysokiej jakości oddala się od głównego problemu badawczego i pełni raczej funkcję kontekstową niż analityczną.

W rozdziale III w sposób bardzo systematyczny opisana została geneza, przebiegu procesu uchwalenia oraz implementacji Dyrektywy NIS (2016/1148) do polskiej ustawy o krajowym systemie cyberbezpieczeństwa. Rozdział zawiera bogate odniesienia do dokumentów źródłowych: rezolucji UE, komunikatów Komisji, opinii Europejskiego Inspektora Ochrony Danych, materiałów sejmowych, stanowisk rządu RP, a także aktów prawnych i ich projektów. Ta część pracy przybiera więc charakter analizy prawniczej z elementami rekonstrukcji procesu legislacyjnego. Niestety w wielu miejscach rozdział przyjmuje postać szczegółowego streszczenia aktów prawnych i ich projektów, te części mogłyby zostać skrócone na rzecz bardziej syntetycznych wniosków. W tej części pracy Autor wskazuje na znaczenie opisywanych aktów pranych (dyrektywy i ustawy), lecz nie dokonuje pogłębionej oceny ich skuteczności, np. czy wykreowany przez nie system faktycznie poprawił bezpieczeństwo cyfrowe, jakie są jego braki, jak reagują podmioty zobowiązane. Niestety brak jest krytycznej oceny opisywanych mechanizmów wdrożeniowych. Rozdział kończy się syntetycznym podsumowaniem, ale nie formułuje wyraźnych wniosków ani oceny skuteczności systemu. Mimo dużej erudycji, zabrakło autorskiego stanowiska w kwestii adekwatności przyjętych rozwiązań prawnych do realnych potrzeb sektora cyfrowego. W tej części pracy problem dostawców usług cyfrowych także pojawia się marginalnie głównie w kontekście kategorii podmiotów objętych obowiązkami. W efekcie rozdział stanowi raczej tło prawne niż analizę tematu tytułowego pracy.

Rozdział IV zawiera analizę przepisów ustawy o krajowym systemie cyberbezpieczeństwa. Autor bardzo szczegółowo omawia zakres podmiotowy ustawy, ze szczególnym uwzględnieniem dostawców usług cyfrowych jako odrębnej kategorii. Przedstawia tam też przykłady problematycznych przypadków m.in. wyszukiwarki tematyczne czy agregatory cen co świadczy o dużym stopniu szczegółowości tej części pracy. Autor bardzo trafnie opisuje koncepcję „light touch" zastosowaną wobec dostawców usług cyfrowych w Dyrektywie NIS i polskiej ustawie pokazując jej genezę, *ratio legis* oraz praktyczne skutki. W części poświęconej art. 17–18 u.k.s.c. Autor szczegółowo analizuje zakres obowiązków dotyczących m.in. zarządzania ryzykiem, obsługi incydentów, raportowania, współpracy z operatorami usług kluczowych czy przekazywania danych osobowych. Wskazuje także problemy interpretacyjne. To bardzo wartościowa, praktyczna i rzadko spotykana w literaturze prawniczej analiza.

Rozdział V stanowi naturalne rozwinięcie analiz dogmatycznych poczynionych we wcześniejszych rozdziałach, jest to najbardziej praktyczny i aplikacyjny fragment całej pracy Autor omawia w nim praktyczną warstwę wdrażania nałożonych przez przepisy obowiązków, wskazując na wynikające z tego normy, standardy i wytyczne np. ISO/IEC 27001, 27002, 27032 oraz standardy dla usług chmurowych. Szczególnie cennym spostrzeżeniem Autora jest tu postulowana przez niego konieczność łączenia wymogów prawnych z dobrymi praktykami technicznymi. Autor trafnie wskazuje, że analizowane przepisy są zbyt ogólne, by przedsiębiorcy mogli łatwo ustalić, jakie działania faktycznie spełniają ustawowe obowiązki. W tym kontekście proponuje stosowanie elastycznych narzędzi zarządzania bezpieczeństwem i odwołuje się do zasad proporcjonalności i „light touch" z Dyrektywy NIS. W mojej ocenie niestety w tej części pracy brakuje prób odpowiedzi na pytanie, czy opisywane standardy faktycznie pozwalają na osiągnięcie celu ustawy, i jakie są ich ograniczenia. W aspekcie prawno porównawczym sekcja o Francji i Niemczech jest dobrze rozwinięta, omówienie systemu brytyjskiego jest niestety skrócone i mniej analityczne. Brak też odniesienia do systemów spoza UE, które mogłyby zilustrować inne podejścia regulacyjne (np. USA, Kanada). Rozdział kończy się raczej opisowym zebraniem informacji, niż klarownymi wnioskami o skuteczności opisywanych rozwiązań prawnych lub proponowanymi kierunkami ich zmian.

Wnioski

Przechodząc do oceny zawartości merytorycznej pracy stwierdzić należy, że oceniana rozprawa jest oryginalnym dziełem, wyraźnie wzbogacającym dorobek polskiej nauki w obszarze prawa nowych technologii oraz nauk o bezpieczeństwie. Lektura pracy daje dowód na to, że jej Autor jest inteligentnym, kompetentnym badaczem, który w polu swoich dociekań porusza się z dużą swobodą, prezentując bardzo dobrą znajomość analizowanej problematyki. Autor w toku swych dociekań przyjmuje krytyczne stanowisko zarówno wobec źródeł, jak również wobec opinii innych autorów. Poglądy te analizuje i poddaje w wątpliwość, podziela, bądź odrzuca, jeśli nie wytrzymują krytyki. Praca dowodzi dużej wiedzy Autora oraz jego wysokiej sprawności intelektualnej. Nowość naukowa recenzowanej publikacji przejawia się w zawężeniu pola badawczego do specyficznej grupy podmiotów – dostawców usług cyfrowych – które dotychczas nie były przedmiotem pogłębionej analizy w literaturze polskiej. Większość wcześniejszych opracowań skupiała się bowiem na operatorach usług kluczowych lub na ujęciach ogólnych dotyczących bezpieczeństwa teleinformatycznego. Dr. Porzeżyński wypełnia tę lukę, tworząc pierwsze w polskim

piśmiennictwie systematyczne ujęcie pozycji prawnej dostawców usług cyfrowych w kontekście obowiązków regulacyjnych, technicznych i organizacyjnych. Wkład Autora w rozwój dyscypliny naukowej przejawia się również w zastosowaniu podejścia interdyscyplinarnego, łączącego metodologię nauk prawnych (analiza dogmatyczna i komparatystyczna) z elementami nauk o bezpieczeństwie i nauk technicznych. W ten sposób monografia wnosi istotny wkład do praktycznej interpretacji przepisów poprzez ich odniesienie do rzeczywistych mechanizmów zarządzania ryzykiem i bezpieczeństwem w sektorze cyfrowym. Wysiłek badawczy, który zainwestował Habilitant zaowocował stworzeniem wartościowego opracowania naukowego wzbogacającego dorobek polskiej doktryny prawa posiadającego jednocześnie praktyczny wymiar aplikacyjny.

Osiągnięcie naukowe Habilitanta, którym jest opisywana wyżej monografia napisane jest bez błędów merytorycznym, reprezentuje wysoki poziom merytoryczny i znacząco wzbogaca dorobek polskiej nauki prawa, jako takie zasługuje na pozytywną ocenę. Postawione w rozprawie habilitacyjnej tezy zostały ujęte prawidłowo oraz w sposób logiczny dowiedzione. Forma i treść pracy pozwalają twierdzić, że Autor posiada umiejętność samodzielnego identyfikowania problemów badawczych, ich usystematyzowania oraz rozwiązywania. Poprawna pod względem metodologicznym oraz merytorycznym analiza poszczególnych zagadnień objętych tematem pracy niewątpliwie istotnie poszerzyła dotychczasowy stan wiedzy. Biorąc pod uwagę wagę dociekań, ich rozmiar oraz ich użyteczność stwierdzić należy, że wymienione osiągnięcie naukowe stanowi znaczny wkład Habilitanta w rozwój dyscypliny naukowej.

Ocena pozostałego naukowego dorobku publikacyjnego Habilitanta

Uwagi ogólne

Po uzyskaniu stopnia naukowego doktora nauk prawnych Habilitant opublikował prace naukowe na co składają się:

a) monografia pt. M. Porzeżyński, *Cyberbezpieczeństwo dostawców usług cyfrowych*, Instytut Wydawniczy EuroPrawo, Warszawa 2021. (275 s.);

b) autorskie artykuły naukowe (11) z czego 2 to publikacje współautorskie;

c) rozdziały w opracowaniach zbiorowych (15), z czego tylko jeden z nich to opracowanie współautorskie;

d) Habilitant jest także redaktorem naukowym 1 publikacji naukowej.

Łącznie jest to 28 publikacji naukowych (opublikowanych po doktoracie), zauważyć należy, że jest to spory dorobek naukowy, który został stworzony przez Habilitanta na przestrzeni ostatnich 8 lat, dodatkowo zauważyć należy, że tylko 3 z tych publikacji ma charakter współautorski. W tym miejscu odnotować należy także bogatą działalność publikacyjną jaką Habilitant zrealizował jeszcze przed doktoratem (5 artykułów naukowych i 7 rozdziałów w monografiach naukowych oraz opublikowana rozprawa doktorska) – co łącznie daje 41 publikacji naukowych.

Tematyka tworzonych przez Autora opracowań naukowych jest bardzo różnorodna i obrazuje szeroki wachlarz zainteresowań naukowych Habilitanta. Znacząca większość opublikowanych artykułów naukowych Habilitanta (opublikowanych po doktoracie) wydana została w czasopismach naukowych znajdujących się na ministerialnej liście:

- Cybersecurity and Law -70 punktów – 1 artykuł;
- Studia Iuridica -100 punktów (Scopus) - 2 artykuły;
- Państwo i Prawo – 70 punktów -1 artykuł;
- Przegląd Prawniczy Uniwersytetu Warszawskiego -70 punktów - 1 artykuł;
- Palestra – 40 punktów - 1 artykuł;
- artykuły w czasopiśmie z spoza listy MNiSW – 5 artykułów.

Na szczególną uwagę zasługuje rozdział w monografii pt „The Future of Consumer Protection and Regulation on Energy Market", wydany w prestriżowym wydawnictwie Routledge (wydawnictwo z poziomu II ministerialnej listy) w ramach serii Routledge Handbook of Consumer Protection in Energy Markets (red. T. Hunter, M. Kraśniewski, M. Czarnecka, J. Malinauskaite, Routledge, Londyn 2024).

Jak widać z powyższego zestawienia Habilitant publikował swoje teksty w renomowanych polskich oraz zagranicznych czasopismach/wydawnictwach naukowych. Wymagania jakie współcześnie stawia się przed habilitantami są dość wysokie, dla oceny dorobku naukowego znaczenie mają m. in. wskaźniki dotyczące cytowalności. Na stronie Google Scholar indeksacji podlegają tylko te publikacje Habilitanta, które opublikowane zostały od roku 2018 r. Wskaźniki naukometryczne wyliczone więc na tej stronie uwzględniają jedynie publikacje z ostatnich lat (od 2018 do 2025). Całkowita liczba cytowań to 10, Indeks Hirscha: 2. Z uwagi jednak, że wyniki Google Scholar dotyczą jedynie lat 2018-2025 a Habilitant publikuje od roku 2013 uznać należy, iż te wartości nie są miarodajne dla oceny dorobku naukowego Habilitanta.

Stworzone przez Habilitanta opracowania naukowe pogrupować można w ramach czterech różnych pól tematycznych takich jak: prawo nowych technologii, ochrony danych

osobowych, własności intelektualnej oraz cyberbezpieczeństwa. Są to obszary analizowane z perspektywy europejskiego i polskiego porządku prawnego, często w kontekście społecznych skutków transformacji cyfrowej.

Ocena pozostałych osiągnięć Habilitanta

Habilitant obecnie jest zatrudniony na stanowisku adiunkta na Wydziale Administracji i Nauk Społecznych Politechniki Warszawskiej, Zakład Prawa Administracyjnego i Nauki o Politykach Publicznych, od 2024 r. pełni funkcję Prodziekana ds. Studenckich, wykonuje także zawód radcy prawnego. W latach 2013 – 2021 był zatrudniony na Uczelni Łazarskiego w Warszawie, na Wydziale Prawa Uniwersytetu SWPS w Warszawie, na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego.

Habilitant był kierownikiem 5 zrealizowanych grantów naukowych:

1. Grant na projekt naukowy realizowany na Uniwersytecie w Turynie (Dipartamento di Giurisprudenza, Turyn, Włochy) pod kierunkiem prof. Ugo Pagallo (4.2024) – kierownik projektu;
2. Grant na projekt naukowy ze środków Politechniki Warszawskiej umożliwiający odbycie kwerendy bibliotecznej w European University Institute we Florencji (4-5.2023) – kierownik projektu;
3. Grant na projekt naukowy w konkursie MINIATURA na realizację działania naukowego „Prawne i etyczne ograniczenia wykorzystania danych biometrycznych w Unii Europejskiej i w Polsce" na podstawie decyzji Dyrektora Narodowego Centrum Nauki nr. DEC2021/05/X/HS5/00760. Projekt realizowany na Uniwersytecie w Turynie (Dipartamento di Giurisprudenza) pod kierunkiem prof. Ugo Pagallo (3.2022) – kierownik projektu;
4. Grant badawczy ze środków Politechniki Warszawskiej umożliwiający odbycie kwerendy bibliotecznej w Max Planck Institute of Comparative Public Law and International Law w Heidelbergu (12.2021 r.) – kierownik projektu;
5. Grant na projekt opracowania programu i materiałów do zajęć dydaktycznych „Introduction to International and European Intellectual Property Law" dla studentów studiów doktoranckich kierunków technicznych w programie Smart Education for Engineering Doctors (SEED) Internalization od Doctoral Schools STER (12.2021) – kierownik projektu.

Obecnie jest także w trakcie realizacji 4 kolejnych grantów naukowych jako kierownik projektu w tym m. in. grantu uzyskanego od Google.org w wysokości $ 892 751 (ok. 3 625 200 zł) na projekt Google Cybersecurity Seminars.

Po doktoracie Habilitant wziął udział i wygłosił referaty na 21 konferencjach naukowych (15 krajowych oraz 6 konferencjach zagranicznych), jest członkiem następujących polskich i zagranicznych stowarzyszeń naukowych i akademickich:

1. Członek Polskiego Towarzystwa Naukowego Prawa Prasowego (od 2017 r.);
2. Dyrektor Instytutu Badań nad Prawnymi Aspektami Nowych Technologii – Future Institute (od 2016 r.);
3. Członek założyciel Stowarzyszenia Prawa Nowych Technologii (od 2019 r.);
4. Członek MIT Technology Review Global Panel (od 2019 r.);
5. Członek European AI Alliance przy Komisji Europejskiej (od 2018 r.);
6. Członek International Association of Young Lawyers (od 2018 r.);
7. Członek European LegalTech Association (od 2017 r.);
8. Członek International Association for Artificial Intelligence and Law (od 2016 r.);
9. Ekspert Fundacji im. Lesława Pagi ds. Innowacji (2015/2016);

Habilitant wziął udział w następujących zagranicznych wyjazdach naukowych:

1. Uniwersytet w Turynie (Turyn, Włochy)- wyjazd naukowy pod kierunkiem prof. Ugo Pagallo i kwerenda biblioteczna (12.05-06.06.2024 r.; 26 dni);
2. European University Institute we Florencji (Florencja, Włochy)- wyjazd naukowy i kwerenda biblioteczna (30.04-13.05.2023 r.; 14 dni);
3. Uniwersytet w Turynie (Turyn, Włochy)- wyjazd naukowy pod kierunkiem prof. Ugo Pagallo i kwerenda biblioteczna (03-04.2022 r.; 15 dni);
4. Max Planck Institute for Comparative Public Law and International Law w Heidelbergu (Heidelberg, Niemcy)- wyjazd naukowy i kwerenda biblioteczna (09-10.2021 r.; 14 dni).

Odnotowania wymaga bogata współpraca Habilitanta z sektorem gospodarczym, pełnił on m. in funkcje: Członka Rady Nadzorczej Hydra Games S.A. (obecnie Eneida Games S.A.) – od kwietnia 2022 r.; Wiceprezes Zarządu La Familia S.A. - od kwietnia 2022 r.; Członka Rady Nadzorczej 4EST S.A. - od czerwca 2021 r.; Prezesa Zarządu CYPHER LYNX Sp. z o. o. -, od marca 2021 r. do czerwca 2022 r.; Członka Rady Nadzorczej Not So Boring Company S.A. -, od grudnia 2020 r. oraz Członka Rady Nadzorczej Unseen Silence S.A. - od października 2020 r.

Jako członek zespołów eksperckich lub konkursowych Habilitant podejmował działanie m. in. w ramach:

- Zespołu ds. Prawa Nowych Technologii na Politechnice Warszawskiej,

- Zespołu Politechniki Warszawskiej i Naczelnej Rady Adwokackiej ds. standardów cyberbezpieczeństwa dla adwokatury,

- Zespołu ekspertów przy Ministerstwie Cyfryzacji (w latach 2020-2022) w ramach grupy roboczej ds. cyberbezpieczeństwa tj. zespole ds. edukacji w cyberbezpieczeństwie oraz zespole ds. certyfikacji w cyberbezpieczeństwie – CertiSecPL.

Podsumowanie

Wyrażam przekonanie, że należy pozytywnie ocenić dokonania dr Marka Porzeżyńskiego zarówno na polu nauki, dydaktyki jaki i popularyzacji nauki. Wypowiedzi naukowe Habilitanta zawsze reprezentowały wysoki poziom merytoryczny, dotyczyły bardzo różnorodnych zagadnień odnoszących się do wciąż aktualnych oraz ważnych z naukowego punktu widzenia zagadnień, większość z nich ma charakter oryginalny i stanowi znaczący wkład w rozwój dyscypliny naukowej. Różnorodność zagadnień, których dotyczą publikacje Habilitanta świadczą o jego erudycji. Na szczególne podkreślenie zasługuje jego aktywność w uzyskiwaniu i realizacji grantów naukowych, oraz jego cztery, kilkunastodniowe starze naukowe w zagranicznych jednostkach naukowych. Z tych względów całokształt dorobku dr Marka Porzeżyńskiego należy ocenić pozytywnie.

Konkluzja recenzji

Mając na uwadze treść art. 219 ust. 1 ustawy z dnia 11 marca 2022 r. Prawo o szkolnictwie wyższym stwierdzam, że:

- Habilitant posiada stopień doktora;

- Habilitant posiada w dorobku, opisane i scharakteryzowane powyżej, osiągnięcia naukowe stanowiące znaczny wkład w rozwój dyscypliny nauki prawa w tym m. in. monografię pt „ „Cyberbezpieczeństwo dostawców usług cyfrowych”, Warszawa 2021, wydanej przez Instytut Wydawniczy EuroPrawo Sp. z o.o., ISBN: 978-83-7627-209-2. Monografia ta jest rozprawą naukową wydaną przez wydawnictwo, które w roku opublikowania monografii w ostatecznej formie było ujęte w wykazie sporządzonym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit.b ustawy Prawo o szkolnictwie wyższym.

- Habilitant wykazuje się istotną aktywnością naukową realizowaną w więcej niż jednej uczelni na terenie kraju oraz za granicą.

Jako recenzent, powołany Uchwałą nr 08/05/06/2025 Rady Naukowej Uniwersytetu Vizja z dnia 5 czerwca 2025 r. w sprawie powołania komisji habilitacyjnej w postepowaniu o nadanie stopnia doktora habilitowanego dr Markowi Porzeżyńskiemu w dziedzinie nauk społecznych w dyscyplinie nauki prawne, wyrażam przekonanie, że Habilitant spełnia wymogi określone w art. 219 ust. 1 ustawy z dnia 11 marca 2022 r. Prawo o szkolnictwie wyższym **(**Dz.U.2024.1571 t.j.**)** warunkujące nadanie stopnia doktora habilitowanego.

Uwzględniając powyższe oceny wnioskuję o dopuszczenie wniosku dr Marka Porzeżyńskiego do dalszych etapów postepowania habilitacyjnego.

Grzegorz Tylec

Prof. ucz. dr hab. Grzegorz Tylec