Dr hab. Arkadiusz Bereza, prof. UMCS
Katedra Prawa Informatycznego i Zawodów Prawniczych
Instytut Nauk Prawnych
Wydział Prawa i Administracji
UMCS w Lublinie

Recenzja

rozprawy habilitacyjnej Pana dra Marka Porzeżyńskiego pt. *„Cyberbezpieczeństwo dostawców usług cyfrowych"*, Warszawa 2021 (Instytut Wydawniczy EuroPrawo), ss. 275 oraz Jego aktywności naukowej, sporządzona w ramach wszczętego postępowania o nadanie stopnia doktora habilitowanego w dziedzinie nauk społecznych, w dyscyplinie nauki prawne.

Stopień doktora habilitowanego nadaje się osobie, która zgodnie z art. 219 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2023 r. poz. 742 ze zm.) – dalej: Ustawa posiada stopień doktora (art. 219 ust. 1 pkt 1 Ustawy), posiada w dorobku osiągnięcia naukowe albo artystyczne, stanowiące znaczny wkład w rozwój określonej dyscypliny, w tym co najmniej 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) Ustawy (art. 219 ust. 1 pkt 2 lit a) Ustawy) oraz wykazuje się istotną aktywnością naukową lub artystyczną realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej (art. 219 ust. 1 pkt 3 Ustawy). Ponadto zgodnie z art. 219 ust. 2 Ustawy osiągnięcie, o którym mowa w ust. 1 pkt 2, może stanowić część pracy zbiorowej, jeżeli opracowanie wydzielonego zagadnienia jest indywidualnym wkładem osoby ubiegającej się o stopień doktora habilitowanego.

Pan dr Marek Porzeżyński ukończył studia na kierunku prawo na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego w 2013 r. uzyskując tytuł zawodowy magistra nauk prawnych. Stopień doktora nauk prawnych w zakresie prawa uzyskał dnia

21 grudnia 2016 r. na podstawie uchwały Rady Wydziału Prawa Uniwersytetu SWPS w Warszawie. Podstawą nadania tego stopnia była rozprawa pt. *„Zdolność patentowa programów komputerowych"*, której promotorem był prof. dr hab. Jacek Sobczak, a recenzentami prof. dr hab. Krystyna Szczepanowska-Kozłowska i prof. dr hab. Joanna Sieńczyło-Chlabicz.

Przed uzyskaniem stopnia doktora nauk prawnych Pan Marek Porzeżyński zatrudniony był jako asystent w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego. Później prowadził zajęcia w charakterze wykładowcy na Wydziale Prawa Uniwersytetu SWPS w Warszawie oraz w Uczelni Łazarskiego w Warszawie. Od 2021 r. zatrudniony jest na stanowisku adiunkta w Zakładzie Prawa Administracyjnego i Nauk o Politykach Publicznych na Wydziale Administracji i Nauk Społecznych Politechniki Warszawskiej.

W uczelniach, z którymi był lub jest obecnie związany prowadził zajęcia dydaktyczne: prywatność i prawo ochrony danych osobowych, cyberbezpieczeństwo, prawo własności intelektualnej, prawo autorskie, prawo mediów, ochrona programów komputerowych, prawo sztucznej inteligencji (rozwój sztucznej inteligencji a prawo), podstawy prawne prowadzenia działalności gospodarczej (ekosystem prawny start up'u). Taki wachlarz zajęć, ujętych niewątpliwie w profilu naukowym Habilitanta wskazuje na Jego dużą wiedzę i gotowość do jej stałego poszerzania. Dodatkowo potwierdzają tc odbyte szkolenia oraz uzyskane tytuły i certyfikaty w kraju i za granicą (certyfikat akredytowanego Audytora Wewnętrznego Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z ISO 27001 (2017); tytuł Master of Business Administration po ukończeniu programu studiów MBA, *Innovation and Data Analysis* zorganizowanych przez Instytut Podstaw Informatyki Polskiej Akademii Nauk we współpracy z Woodbury School of Business (akredytacja AACSB) i Utah Valley University (2019); *Certified Information Privacy Professional/Europe* wystawiony przez International Association of Privacy Professionals (2020) oraz AI & Law Summer School organizowany przez European University Institute we Florencji i University of Pittsburgh School of Law (2023). Zwraca uwagę intensywność i systematyczność w zdobywaniu kompetencji Habilitanta w obszarze jego zainteresowań w stosunkowo krótkim czasie po uzyskaniu stopnia doktora.

Habilitant jest zaangażowany w działalność organizacyjną na uczelni, w której jest obecnie zatrudniony. W latach 2020-2024 był rzecznikiem dyscyplinarnym ds. studentów i doktorantów, zaś od 2024 r. pełni funkcję prodziekana ds. studenckich na Wydziale Administracji i Nauk Społecznych Politechniki Warszawskiej. Jest również pełnomocnikiem dziekana ds. ochrony danych osobowych i uczestniczy w pracach różnych zespołów i komisji na szczeblu wydziału i całej uczelni (np. w Komisji Senackiej ds. współpracy z zagranicą). Jest członkiem zespołu badawczego opracowującego zasady cyberbezpieczeństwa Wydziału Administracji i Nauk Społecznych Politechniki Warszawskiej oraz grupy ds. eksploracji i eksploatacji Sztucznej Inteligencji (powołany przez Rektora Politechniki Warszawskiej jako ekspert od własności intelektualnej, ochrony danych osobowych i prawa sztucznej inteligencji). Powyższe wskazuje na aktywny udział w życiu uczelni z wykorzystaniem posiadanej wiedzy i doświadczenia. Pan dr Marek Porzeżyński jest praktykiem, radcą prawnym, którego specjalizacja zawodowa dotycząca własności intelektualnej, nowych technologii, ochrony danych osobowych i cyberbezpieczeństwa nawiązuje do jego zainteresowań naukowych. Uczestniczył również w pracach Grupy Roboczej ds. Cyberbezpieczeństwa przy Ministrze Cyfryzacji w ramach zespołów ds. edukacji w cyberbezpieczeństwie i ds. certyfikacji w cyberbezpieczeństwie. Jest członkiem Polskiego Towarzystwa Naukowego Prawa Prasowego oraz Stowarzyszenia Prawa Nowych Technologii, MIT Technology Review Global Panel, European AI Alliance przy Komisji Europejskiej, International Association of Young Lawyers, European LegalTech Association i International Association for Artificial Intelligence and Law. Liczne wywiady, szkolenia, prelekcje, spotkania i grupy dyskusyjne, w których bierze udział mogą świadczyć o nim jako nauczycielu akademickim popularyzującym naukę.

Habilitant wykazuje się istotną aktywnością naukową realizowaną w więcej niż jednej uczelni, instytucji naukowej, w tym zagranicznej. Wskazują na to wyjazdy naukowe do Uniwersytetu w Turynie, Max Planck Institute of Comparative Public Law and International Law w Heidelbergu, czy European University Institute we Florencji realizowane w ramach programu MINIATURA (pierwszy z nich) lub uczestnictwo w projektach wewnętrznych finansowanych ze środków Politechniki Warszawskiej. Habilitant w dniu sporządzenia wniosku planował kolejne wyjazdy naukowe do Tokio i Turynu. Obecnie pełni funkcję kierownika w projekcie Google Cybersecurity Seminars

oraz jest wykonawcą w jednym z projektów w ramach konkursu OPUS 22 (wniosek pt. *„Nadużycie marki - marka jako nowe dobro osobiste w polskim prawie cywilnym na tle regulacji europejskich i prawa amerykańskiego"*).

Podkreślenia wymaga duża aktywność Habilitanta w konferencjach naukowych, w tym międzynarodowych (40 konferencji, w tym 19 przed uzyskaniem stopnia doktora - wymienionych w załączniku nr 4 do wniosku) o różnej tematyce szczegółowej dotyczącej płaszczyzny nowych technologii, sztucznej inteligencji, cyberbezpieczeństwa czy własności intelektualnej. Wystąpienia (w ostatnim okresie często na zaproszenie organizatorów lub w czasie sesji plenarnej) wystawia tej sferze aktywności naukowej Habilitanta wysoką ocenę.

Pan dr Marek Porzeżyński (wg załącznika nr 4 do wniosku i autoreferatu) opublikował dotychczas 2 monografie (łącznie z recenzowaną monografią habilitacyjną), 22 rozdziały w monografiach naukowych (w tym 7 przed uzyskaniem stopnia doktora) oraz 16 artykułów w czasopismach naukowych (w tym 5 przed uzyskaniem stopnia doktora). Trzy publikacje powstały we współautorstwie, w tym 1 rozdział w monografii (wydanej w wydawnictwie Routledge, Londyn 2024) i 2 artykuły w czasopismach naukowych (w *Cybersecurity and Law 2024*, vol. 11 oraz *Studia Iuridica* 2022, t. 95 – artykuły anglojęzyczne).

Pierwsza monografia będąca publikacją pracy doktorskiej wydana została przez Wydawnictwo C.H. Beck, zaś rozprawa habilitacyjna przez Instytut Wydawniczy EuroPrawo - wydawnictwa naukowe sklasyfikowane na I poziomie wykazu wydawców publikujących recenzowane monografie naukowe wskazane w załączniku do komunikatu Ministra Edukacji i Nauki z dnia 22 lipca 2021 r.

Niektóre rozdziały autorstwa Habilitanta w monografiach wieloautorskich publikowane były w wydawnictwach uczelni z którymi był on związany (Uniwersytet Warszawski, Politechnika Warszawska), ale także w innych wydawnictwach krajowych m. in. Instytut Wydawniczy EuroPrawo (Warszawa), Difin (Warszawa), Laboratorium Wiedzy Artur Borcuch (Kielce), Wolters Kluwer (Warszawa), Towarzystwo Wiedzy Obronnej (Warszawa), a także w wydawnictwach zagranicznych (Londyn, Lwów).

Artykuły Jego autorstwa po uzyskaniu stopnia doktora były publikowane w różnych krajowych czasopismach naukowych (wg kolejności wymienionych we wniosku artykułów): *Cybersecurity and Law, Studia Iuridica, Państwo i Prawo, Przegląd*

Prawniczy Uniwersytetu Warszawskiego, Palestra, Themis Polska Nova, Horyzonty Bezpieczeństwa, Miesięcznik ODO, Miesięcznik Ubezpieczeniowy.

Dane naukometryczne wskazane przez Habilitanta to liczba cytowań jego publikacji - 8 (brak oddzielnego uwzględnienia autocytowań), Indeks Hirscha – 2, zaś punktacja MNiSW – 485 (za okres 2022-2024).

Według ustaleń recenzenta (na dzień sporządzenia recenzji) dorobek naukowy Habilitanta według Scopus References - 1 cytowanie, zaś według Google Scholar (Publish or Perish) wykazuje 24 cytowania, z wyłączeniem autocytowań – 16. Indeks Hirscha był równy 3, z wyłączeniem autocytowań – 2.

Pan Marek Porzeżyński nie ubiegał się dotychczas o nadanie stopnia doktora habilitowanego.

W dorobku Habilitanta można wyodrębnić trzy obszary badawcze, które łączą Jego pasję naukową i doświadczenie zawodowe. Są to:

1) ochrona własności intelektualnej (ze szczególnym uwzględnieniem oprogramowania komputerowego);

2) ochrona informacji, w tym ochrona danych osobowych;

3) cyberbezpieczeństwo.

W każdym z tych obszarów Pan dr Marek Porzeżyński zaznacza swoją obecność naukową, lecz nie w stopniu równomiernym. Nie było to zresztą – tak przyjmuję - Jego zamierzeniem i jest wynikiem jego rozwoju naukowego w kolejności podanych wyżej nurtów badawczych. Ważne jest to, że dorobek naukowy Habilitanta jest różnorodny, chociaż skupia się na zagadnieniach dotyczących nowych technologii i cyberbezpieczeństwa. Z tym związany jest również udział Habilitanta w powstaniu recenzowanego podręcznika akademickiego (*Prawo informatyczne i geoinformacyjne,* red. M. Jankowska i M. Pawełczyk, Warszawa 2021).

Z pierwszym obszarem wiążą się zainteresowania Habilitanta związane z jego rozprawą doktorską, która została opublikowana rok po jej obronie w wydawnictwie C.H. Beck pt. *„Zdolność patentowa programów komputerowych"*, Warszawa 2017. Poruszane w tytule zagadnienie znalazło się w orbicie zainteresowania praktyki, jak i doktryny prawa. Jest to publikacja Habilitanta o najwyższej cytowalności - według Google Scholar (Publish or Perish) 4 cytowania - spośród wszystkich prac wchodzących w skład dorobku naukowego Habilitanta. Postulaty w niej zawarte okazały się pomocne w pracach

legislacyjnych nad zmianami ustawy z dnia 30 czerwca 2000 r. - Prawo własności przemysłowej oraz przy formułowaniu wytycznych Prezesa Urzędu Patentowego RP (dyrektyw interpretacyjnych), chociaż nie ma w nich odesłania do w/w publikacji.

Na szczególną uwagę zasługuje obszar trzeci, w który wpisuje się monografia habilitacyjna pt. *„Cyberbezpieczeństwo dostawców usług cyfrowych"*, Warszawa 2021. To osiągnięcie naukowe jest podstawą wniosku o nadanie stopnia doktora habilitowanego w dziedzinie nauk społecznych, w dyscyplinie: nauki prawne. Tytuł oraz analiza zawartości monografii, opisanych w niej pojęć, instytucji i instrumentów prawnych oraz zastosowanych metod badawczych pozwala na zaliczenie jej do dyscypliny nauki prawne, mimo początkowych wątpliwości, czy nie należy ona do – cechującej się jednak niską konkretnością - dyscypliny nauki o bezpieczeństwie.[1]

Nie oznacza to, że pozostałe osiągnięcia naukowe mają mniejszą wartość, a jedynie to, że pozostają one w związku lub obok głównego nurtu badawczego Habilitanta tworząc łącznie sylwetkę badacza naukowego.

Wybór tematyki monografii habilitacyjnej jest trafny. Zagadnienie to nie było przedmiotem kompleksowych badań i tak szerokiej analizy dotyczącej sytuacji prawnej i wymagań stawianych dostawcom usług cyfrowych w ramach systemu cyberbezpieczeństwa, zwłaszcza w kontekście pytania, czy osiągnięcie minimalnego poziomu cyberbezpieczeństwa podmiotów będzie możliwe za pomocą wprowadzonych już obowiązków. Tezę tę Habilitant zweryfikował negatywnie (s. 13, 22, 250) i wysunął propozycje zmian ustawowych dotyczących cyberbezpieczeństwa dla zapewnienia jego minimalnego poziomu w społeczeństwie (identyfikując się z koncepcją dotyczącą konieczności wprowadzenia minimalnego poziomu cyberbezpieczeństwa, s. 18, 104-105, 108). Wątpliwości budzi brzmienie tytułu monografii. Sugeruje on szersze ujęcie tematu (obejmującego także zagadnienia techniczne i technologiczne towarzyszące urzeczywistnieniu założenia cyberbezpieczeństwa), a przecież Habilitant ograniczył swoje rozważania do *„przedstawienia oraz analizy prawnej problematyki cyberbezpieczeństwa ze szczególnym naciskiem położonym na cyberbezpieczeństwo dostawców usług cyfrowych w Europie i w Polsce"* (s.16). Habilitant stwierdza również, że

[1] Problemy dotyczące zdefiniowania i określenia zakresu przedmiotowego dyscypliny nauki o bezpieczeństwie patrz: M. Lutostański, *Idea wyodrębnienia dyscypliny naukowej „nauki o bezpieczeństwie" i jej konsekwencje*, „Historia i Polityka", 2018, nr 25, s. 9-22.

przeprowadzone badania *„obejmują dogłębną analizę aktów prawnych związanych z tematyką cyberbezpieczeństwa..."* (s. 17), lecz nieco zmarginalizował – tj. pozostawił poza główną osią przeprowadzonej analizy - znaczenie niektórych aktów normatywnych kształtujących całe środowisko prawne cyberbezpieczeństwa. Niemniej fragmenty pracy, w których o nich wspomina, zawierają ciekawe porównania i trafne wnioski. Dotyczy to m. in. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 4.05. 2016 r. z późn. zm.) (RODO), ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t. j. Dz. U. z 2025 r. poz. 1209), a także przepisów dotyczących zarządzania kryzysowego – w tym ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t. j. Dz. U. z 2023 r. poz. 122 z późn. zm.) oraz rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. Nr 83, poz. 542) w zakresie w jakim dotyczą operatorów infrastruktury krytycznej, które mogą bezpośrednio kształtować sytuację prawną dostawców usług cyfrowych, także w obszarze cyberbezpieczeństwa. Być może Habilitant uznał to za zbędne poszukując wyraźnych granic dla swojej analizy objętej rozprawą habilitacyjną, jednakże nie zostało to wprost wyartykułowane.

Monografia została wydana w 2021 r., a więc niektóre twierdzenia czy ustalenia Autora wymagają weryfikacji z uwagi na szybko zmieniające się otoczenie prawne w obszarze cyberbezpieczeństwa. Przyczynę wystąpienia z wnioskiem o wszczęcie postępowania w sprawie nadania stopnia doktora habilitowanego dopiero po czterech latach Habilitant wyjaśnia w autoreferacie. Rozprawę należy ocenić z perspektywy czasu, w którym ona powstała i obowiązującego wtedy stanu prawnego. Habilitant ma tego świadomość, podobnie jak i uzmysławia sobie powstanie nowych wyzwań w obszarze cyberbezpieczeństwa wobec rosnącej dynamiki i skali ataków cybernetycznych, których statystyka z pewnością obiega od oficjalnych danych. Analizowany przez Habilitanta stan prawny zatrzymuje się na dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016 r.) - dyrektywa NIS 1 i etapie wdrożenia jej do polskiego porządku prawnego

w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa i wydanych do ustawy aktach wykonawczych. Z oczywistych względów nie zostały uwzględnione akty wydane później, zmieniające – także z uwagi na rozwój technologiczny i idącą za nim digitalizację gospodarki i życia prywatnego - perspektywę spojrzenia na kwestie odporności podmiotów i ich obowiązków w obliczu ataków cybernetycznych. Niemniej Habilitant dostrzega i analizuje kierunki projektowanych zmian (podrozdział III.4 i s. 129). Dlatego uzupełnia swoje rozważania z kart rozprawy habilitacyjnej m. in. w późniejszej publikacji pt. *Changes introduced by the NIS Directive 2.0 and their potential effects on the cybersecurity labour market*, Cybersecurity and Law 2024, vol. 11, ss. 21-37 (we współautorstwie z Ł. Kulickim) poświęconej wdrożeniu i potencjalnym skutkom dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022 r.). Przepisy te powinny być już wdrożone do polskiego porządku prawnego (zgodnie z art. 41 dyrektywy powinny być stosowane we wszystkich krajach Unii Europejskiej od dnia 18 października 2024 r.), lecz przez długi okres trwała debata (i trwa ona nadal) na temat sposobu ich implementacji, co wiąże się również z odpowiednim przygotowaniem, obowiązkami prawnymi i odpowiedzialnością przedsiębiorców i innych podmiotów krajowych.[2] Implementacja dyrektywy ma nastąpić w drodze uchwalenia projektu zmiany ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa i innych ustaw, który uzyskał akceptację Stałego Komitetu Rady Ministrów na posiedzeniu w dniu 4 września br.

Rozprawa habilitacyjna została podzielona na pięć rozdziałów, wstęp i zakończenie. Rozdziały I i II miały mieć w założeniu charakter wprowadzający do tematu i porządkują pojęcia, terminy i dokumenty urzędowe dotyczące cyberbezpieczeństwa na poziomie międzynarodowym i krajowym. Wątpliwości budzi tytuł rozdziału II „Wprowadzenie do cyberbezpieczeństwa", podczas gdy jego treść dotyczy dokumentów o charakterze opiniodawczym i strategicznym ukierunkowanych na kształtowanie podstaw/ram prawnych systemu cyberbezpieczeństwa (zwłaszcza, że sam Autor we

[2] Szerzej na ten temat patrz: Raport „Incydenty pod kontrolą" dotyczący gotowości organizacji na NIS 2 https://incydentypodkontrola.pl/ [dostęp: 5.10.2025].

Wprowadzeniu potwierdza, że „funkcję wprowadzającą" pełni rozdział I – s. 19). Na marginesie należy podnieść dwie kwestie. W strukturze podrozdziału II.2 pojawiła się dysproporcja - nie wyodrębnia się pojedynczych punktów w podrozdziałach, a połączenie tytułów II.2 i II.2.1. nie powinno sprawić Autorowi trudności. W tytułach podrozdziałów I.2. i I.2.1. użyto sformułowania „pojęcia kluczowe", a bardziej adekwatnym terminem wydaje się „podstawowe pojęcia". „Kluczowe pojęcia"/"Słowa kluczowe" stosuje się w terminologii stosowanej w opracowywaniu artykułów naukowych dla celów pozycjonowania, czy wyszukiwania podstawowych treści.

Odnośnie do treści rozdziału I charakteryzuje się przewagą opisu nad analizą. Wydaje się, że zbyt dużo miejsca poświęcono prezentacji różnych definicji kosztem ich krytycznej oceny i syntezy. Brak jest również wyraźnej konkluzji terminologicznej. Po obszernej analizie różnych definicji brakuje jasnego stanowiska Autora co do preferowanego rozumienia podstawowych pojęć. Wskazanie jednoznacznego kierunku interpretacyjnego niewątpliwie wzbogaciłoby walor poznawczy. W tym kontekście Autor nie dokonuje wystarczającej operacjonalizacji analizowanych pojęć dla potrzeb dalszych badań. Definicje pozostają na poziomie abstrakcyjnym. Brakuje wyraźnego wskazania, jak ustalenia terminologiczne wpływają na dalsze badania.

Określone uwagi rodzą się również po lekturze Wprowadzenia do monografii. Przede wszystkim nie odniesiono się wyraźnie do ram tematu (który jako taki został określony bardzo szeroko). Nie wskazano również na kryterium doboru innych państw UE w ramach metody komparatystycznej (s. 20, 22). Wprowadzenie budzi określone zastrzeżenia metodologiczne. Określono cel badawczy, ale nie sformułowano pytań badawczych (ogólnych, szczegółowych), nie sformułowano w wyraźny sposób hipotez badawczych, czy tez badawczych (niektóre z tych ostatnich można wywieść dopiero z całości treści Wprowadzenia). We Wprowadzeniu nie przedstawiono również dotychczasowego stanu wiedzy oraz literatury przedmiotu w tym konkretnym obszarze badawczym (nie określa tego również dość krótki Rozdział I.1).

Habilitant analizuje podstawy prawne oraz ocenia adekwatność obowiązków nałożonych na dostawców usług cyfrowych (mniej rygorystycznych aniżeli przy operatorach usług kluczowych) i sposobu ich wypełniania dla osiągnięcia założonego celu (rozdział III i IV). Ta część rozprawy zawiera główne rozważania Habilitanta odnoszące

się stricte do tematu rozprawy. Uzupełnia je rozdział V dotyczący sposobu spełniania prawnych wymagań nałożonych na dostawców usług cyfrowych poprzez analizę i sposób praktycznego wykorzystania dokumentów o charakterze norm i wytycznych branżowych (normy wydawane przez Międzynarodową Organizację Normalizacyjną - ISO i dokumenty przygotowane przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa - ENISA).

Należy zaznaczyć, że temat cyberbezpieczeństwa został dookreślony pod względem podmiotowym i obejmuje on analizę aspektów funkcjonowania kategorii podmiotów zaliczanych do dostawców usług cyfrowych. W tym zakresie rozprawa wypełnia lukę w ówczesnym (na 2021 r.) stanie badań, gdyż dotyczy grupy dotychczas pomijanej w głównym nurcie prac naukowych (s. 16). Zatem dokonany przez Habilitanta wybór problematyki badawczej należy uznać za uzasadniony i adekwatny do wymogów stawianych rozprawom habilitacyjnym.

Problematyka monografii do łatwych nie należy, nie tylko z uwagi na analizowane akty normatywne i źródła nie mające takiego charakteru, ale również umieszczenia tego obszaru badawczego na styku różnych dyscyplin. Być może z w/w przyczyn, ta niewątpliwie złożona i wielopłaszczyznowa tematyka, nie cieszyła się dużym zainteresowaniem badaczy. Przyjęte w pracy założenia Habilitant zrealizował z dużą znajomością problematyki, wykazując jednocześnie wysoki poziom kunsztu pisarskiego. Dobre wrażenie robi aparat przypisów oraz wartki nurt narracji (chociaż nie uniknięto powtórzeń). Habilitant wyciągnął uniwersalne wnioski, które należy uznać za poprawne. Rekomendacje dotyczące wzmocnienia zabezpieczeń cybernetycznych technologią blockchain czy wsparciem cyberbezpieczeństwa technologią uczenia maszynowego (s. 253) - patrząc z perspektywy aktualnego stanu wiedzy - są bezsprzecznie trafne. Tym zagadnieniom dostrzeżonym przez Autora obecnie poświęca się wiele uwagi.[3]

---

[3] Do takich pozycji w literaturze należą m. in. Saleh, A. (2024). Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review. *Blockchain: Research and Applications*. https://doi.org/10.1016/j.bcra.2024.100193; Ullah, Z., Waheed, A., Mohmand, M., Basar, S., Zareei, M., & Granda, F. (2024). AICyber-Chain: Combining AI and Blockchain for Improved Cybersecurity, *IEEE Access*, 12, 142194-142214. https://doi.org/10.1109/ACCESS.2024.3463976; Alevizos, L., & Ta, V. (2024). Automated Cybersecurity Compliance and Threat Response Using AI, Blockchain & Smart Contracts. *ArXiv*, abs/2409.08390. https://doi.org/10.1007/s41870-024-02324-9; Mohamed, S., M, N., N, T., J, E., & Hermansyah, S. (2025). AI and Blockchain in Cybersecurity: A Sustainable Approach to Protecting Digital Assets. *Jurnal Ilmiah Informatika dan Komputer*. https://doi.org/10.69533/1hh4he43; Beretas, C., & Davalas, A. (2024). Bridging AI Innovation and Cybersecurity: Generative AI's Contribution to NIS2

Nie jest to jednak pozycja przystępna w odbiorze dla potencjalnego czytelnika, który nie jest zainteresowany zagadnieniami prawnymi z zakresu cyberbezpieczeństwa (krąg adresatów wskazano na s. 253-254, stąd m. in. uwaga dotycząca szerszego zaprezentowania w/w aktów prawnych tworzących złożony system rozwiązań dotyczących cyberbezpieczeństwa). Niestety monografia nie jest wykorzystywana w literaturze prawniczej, być może z przyczyny szybkich zmian stanu prawnego i pojawiających się nowych wyzwań w cyberprzestrzeni. Mimo starannej kwerendy obejmującej publikacje prawnicze o różnym charakterze (książki, leksykony, rozdziały w monografiach, artykuły) z okresu 2021-2025 nie znalazłem cytowań recenzowanej monografii. Pozycją odwołującą się do niej jest natomiast rozprawa doktorska: J. Kiera, *Wojna informacyjna w polityce zagranicznej Federacji Rosyjskiej wobec Polski w latach 2010-2022,* Katowice 2025, Wydział Nauk Społecznych Instytut Nauk Politycznych Uniwersytetu Śląskiego.

Podstawową metodą stosowaną przez Autora jest metoda formalno-dogmatyczna oraz analiza i krytyka piśmiennictwa oraz orzecznictwa. Uzupełniająco - metoda komparatystyczna i statystyczna. Dobór metod badawczych należy uznać za właściwy i adekwatny zarówno ze względu na cel, jak i przedmiot badawczy rozprawy habilitacyjnej. Sposób posługiwania się w/w metodami przez Autora dla przeprowadzenia analizy zagadnień związanych z opisywaną problematyką jest prawidłowy i świadczy o Jego dobrym przygotowaniu merytorycznym.

Podstawę recenzowanego opracowania stanowią zebrane i przeanalizowane przez Autora akty prawne (61 pozycji), różnego rodzaju dokumenty urzędowe, stanowiska, wytyczne, zalecenia i opinie (83 pozycje) oraz literatura (186 pozycji w większości obejmujących literaturę przedmiotu). Niektóre z w/w pozycji zostały niezbyt trafnie umieszczone w strukturze bibliografii rozprawy (np. pozycje 1-3 zawierające akty prawne z innych państw w *Pozostałych dokumentach*). Kwerendę biblioteczną na potrzeby rozprawy Habilitant prowadził m. in w ramach realizowanego przez niego projektu naukowego sfinansowanego ze środków Politechniki Warszawskiej w czasie

---

Compliance. *International Journal of Regional Development.* https://doi.org/10.5296/ijrd.v11i2.22486; Bako, N., Ozioko, C., Sanni, I., & Oni, O. (2025). The Integration of AI and blockchain technologies for secure data management in cybersecurity. *World Journal of Advanced Research and Reviews.* https://doi.org/10.30574/wjarr.2025.25.3.0784.

wyjazdu naukowego do Max Planck Institute of Comparative Public Law and International Law w Heidelbergu.

Dokonując analizy wykorzystanej literatury wskazać można dodatkowe pozycje, lecz uznaję to za zbędne wobec szerokiego wykorzystania przez Habilitanta poglądów doktryny oraz z uwagi na fakt, że wobec szerokiego spektrum poruszanych zagadnień dotyczących cyberbezpieczeństwa wykorzystanie wszystkich dostępnych źródeł nie jest konieczne.

Zaznaczam, że wskazane w treści recenzji uwagi mają charakter porządkujący lub uzupełniający (w pewnym zakresie także dyskusyjny) i nie umniejszają one zalet merytorycznych monografii habilitacyjnej.

Konkluzja

Tematyka zawarta w przedstawionej do oceny monografii nie była dotychczas w takiej formule kompleksowo opracowana w literaturze naukowej. Praca stanowi znaczny wkład Autora w badania nad aspektami prawnymi cyberbezpieczeństwa (choć jak wyrażono to w treści recenzji stan badań powinien zostać bardziej wnikliwie zakreślony). Monografia, pomimo określonych mankamentów, zawiera szereg ustaleń, dokonanych po przeprowadzeniu dość rzetelnej analizy aktów prawnych i literatury przedmiotu, dających nie tylko dowód znajomości poruszanej przez Autora problematyki, ale przede wszystkim wypełniających lukę w dotychczasowym stanie badań. Monografia stanowi więc oryginalne pod względem treści i formy dzieło, które w sposób istotny wzbogaca naszą wiedzę i przyczynia się do rozwoju nauki.

Tym samym stwierdzam, że przedstawione do oceny osiągnięcie naukowe monografia pt. *„Cyberbezpieczeństwo dostawców usług cyfrowych"*, Warszawa 2021, (Instytut Wydawniczy EuroPrawo), ss. 275 autorstwa Pana Marka Porzeżyńskiego stanowi znaczny wkład w rozwój dyscypliny nauki prawne (art. 219 ust. 1 pkt 2 lit. a) Ustawy).

Po uzyskaniu stopnia doktora Pan Marek Porzeżyński opublikował 28 publikacji naukowych (2 monografie – w tym jedna stanowi publikację pracy doktorskiej, 15 rozdziałów w monografiach i 11 artykułów) oraz była współredaktorem naukowym jednej pracy naukowej. Uczestniczył – najczęściej w formie czynnej - w 21 konferencjach

naukowych, w tym o charakterze międzynarodowym. Uczestniczył w wyjazdach naukowych do Uniwersytetu w Turynie, Max Planck Institute of Comparative Public Law and International Law w Heidelbergu, czy European University Institute we Florencji realizowanych w ramach programu MINIATURA lub projektów wewnętrznych finansowanych ze środków Politechniki Warszawskiej.

Aktywność naukową umiejętnie łączył z szeroką działalnością dydaktyczną oraz wykonywaniem obowiązków organizacyjnych, pełniąc wskazane w recenzji funkcje (w tym funkcję prodziekana ds. studenckich) oraz zasiadając w różnych gremiach (komisjach, zespołach i grupach roboczych) na Politechnice Warszawskiej. Tym samym Pan Marek Porzeżyński wykazuje się istotną aktywnością naukową realizowaną w różnych uczelniach wyższych tj. w Politechnice Warszawskiej, uczelniach, w których był poprzednio zatrudniony oraz zagranicznych ośrodkach akademickich w ramach wyjazdów naukowych (art. 219 ust. 1 pkt 3 Ustawy).

Wobec powyższego pozytywnie oceniam spełnienie przesłanek wynikających z art. 219 ust. 1 pkt 2 lit. a) i pkt 3 Ustawy oraz wnoszę o dopuszczenie Pana doktora Marka Porzeżyńskiego do dalszych etapów postępowania w sprawie nadania stopnia doktora habilitowanego.

Lublin, 16 października 2025 r.

dr hab. Arkadiusz Bereza, prof. UMCS