Warszawa, 17.10.2025 r.

dr hab. Jakub J. Szczerbowski, prof. UŁ
Zakład Metodologii Prawoznawstwa i Badań Interdyscyplinarnych
Instytut Badań Prawnoporównawczych i Interdyscyplinarnych
Wydział Prawa i Administracji
Uniwersytet Łódzki

Recenzja

Niniejsza recenzja sporządzona jest na podstawie przepisu art. 221 ust. 8 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (dalej: p.s.w.n.) w postępowaniu w sprawie nadania stopnia doktora habilitowanego wszczętego na wniosek **dr Marka Porzeżyńskiego** (dalej: Habilitant). Wniosek z załącznikami doręczono mi 16.9.2025 r.

W pierwszej kolejności należy wskazać, że celem recenzji, zgodnie z dyspozycją przepisu art. 221 ust. 8 p.s.w.n., jest ocena czy osiągnięcia naukowe osoby ubiegającej się o stopień doktora habilitowanego odpowiadają wymaganiom określonym w art. 219 ust. 1 pkt 2 p.s.w.n. Zgłoszone przez Habilitanta osiągnięcia zawierają monografię naukową, co oznacza konieczność jej oceny pod względem tego, czy a) stanowi znaczny wkład w rozwój określonej dyscypliny oraz b) czy została wydana 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 p.s.w.n. Pozostałe osiągnięcia podlegają ocenie pod względem znaczenia dla dyscypliny.

1. Monografia

Zgłoszona w trybie w art. 219 ust. 1 pkt 2 lit. a p.s.w.n. monografia to M. Porzeżyński, *Cyberbezpieczeństwo dostawców usług cyfrowych*, Warszawa 2021, ISBN: 978-83-7627-209-2.

1.1. Ocena merytoryczna

Monografia *Cyberbezpieczeństwo dostawców usług cyfrowych* jest pierwszym kompleksowym opracowaniem problematyki, która zagościła w pełni w krajowym systemie prawnym wraz z uchwaleniem ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa implementującej Dyrektywę 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. Wybór tematyki przez Habilitanta należy zatem uznać za bardzo trafny pod kątem naukowym, a jednocześnie społecznie istotny.

Praca składa się z wprowadzenia, pięciu rozdziałów oraz zakończenia. Redakcja wprowadzenia nie należy do mocnych stron pracy, jest ono zbyt długie i nie w pełni ustrukturyzowane. Wskazuje ono cele pracy oraz stawia hipotezę, że „krajowy system cyberbezpieczeństwa w obecnej formie nie przyczynia się do znaczącego podniesienia poziomu cyberbezpieczeństwa w ogólności" (s. 22). Postawienie hipotezy takiej treści oceniam pozytywnie, jest ona wystarczająco precyzyjna i wyraźna, aby determinować zakres badań oraz treść relacjonującego je wywodu.

We wprowadzeniu zostały także opisane stosowane w pracy metody, a właściwie metoda formalno-dogmatyczna. Co prawda wskazano także metodę komparatystyczną, ale jej opis wskazuje, że chodzi także o metodę formalno-dogmatyczną, a jedynie przedmiotem badań są prawa obce. Wskazano także, że „dopuszczono możliwość skorzystania z metodologii mającej znaczenie dla nauk o bezpieczeństwie i nauk technicznych w szczególności w postaci metody empirycznej", ale już brak wskazania, czy metody te zastosowano, a jeżeli tak, to jakie. Pozostawia to pewien niedosyt w pracy, która stawia przed sobą tak poważne cele.

Rozdział I „Cyberbezpieczeństwo jako przedmiot zainteresowań naukowy i badawczych" stanowi naturalną konsekwencję interdyscyplinarnego charakteru pracy. Skupia się on na wyjaśnianiu pojęć oraz wprowadzeniu w problematykę nauki o cyberbezpie-

czeństwie. Rozdział ten podejmuje próbę uporządkowania nawarstwiających się różnic w rozumieniu pojęć wykorzystywanych w pracy i wydaje się niezbędny dla dalszej lektury. Rozdział ten napisany jest zasadniczo dobrze, chociaż zdarzają się tam pewne błędy. Przykładowo, wskazano, że do popełnienia przestępstwa komputerowego z biegiem czasu przestał być potrzebny komputer (s. 34), czego dowodem ma być użycie urządzeń takich jak inteligentne telefony. Z takim tokiem rozumowania nie sposób się zgodzić, albowiem smartfon ma wszelkie cechy niezbędne do nazwania go komputerem (wykonuje obliczenia, posiada pamięć, można go programować). Życzliwie przyjmuję, że chodzi tu o specyficzną dla przedmiotu definicję konstrukcyjną pojęcia komputera – chociaż nie widzę praktycznego sensu takiego zabiegu w pracy tworzonej w tak silnie technicznym obszarze.

Rozdział II „Wprowadzenie do cyberbezpieczeństwa" zawiera krytyczny rys historyczno-instytucjonalny rozwoju tej dziedziny regulacji. Konstrukcja rozdziału jest trafna, wychodzi on od działań najstarszych i o najszerszym zasięgu geograficznym, a kończy na działaniach najnowszych w kraju. Odpowiedni także jest poziom szczegółowości omówienia – co biorąc pod uwagę ilość informacji zawartą w dokumentach rozmaitych organizacji, jest dużą zaletą.

Habilitant omawia działania ONZ, w tym rezolucje ZO ONZ nr 45/121 (14 grudnia 1990 r.), która dotyczyła przestępstw popełnianych z użyciem komputerów i kładła nacisk na wprowadzenie do krajowych porządków prawnych odpowiednich norm, ZO ONZ nr 55/63 (2001 r.), która kładła nacisk na potrzebę współpracy organów ścigania, ZO ONZ nr 56/121 (2002 r.) dotyczącą eliminacji możliwości bezpiecznego schronienia dla sprawców nadużyć technologii informatycznych, ZO ONZ nr 56/121 (2002 r.) dotyczącą prawa do prywatności, ZO ONZ nr 58/199 (2004 r.) dotyczącą kultury cyberbezpieczeństwa i ochrony infrastruktury krytycznej. Następnie przechodzi do działań podejmowanych przez NATO, sprawnie relacjonując wysiłki podejmowane w tym zakresie, zwłaszcza skupiając się na latach po roku 2007. Kolejno omawia instytucje i konwencje w ramach systemu Rady Europy, a następnie, obszernie, omawia akty i działania organów Unii Europejskiej. Obszerny

rys dotyczący instytucji o międzynarodowym polu działania znacząco wzbogaca pracę i pozwala umieścić szczegółowe rozważania w szerokim kontekście.

W tym samym rozdziale Habilitant omawia działania krajowe od rządowego programu z lat 2009-2011 do działań podejmowanych do publikacji monografii. Habilitant nie kryje negatywnego stosunku do niektórych inicjatyw podejmowanych przez kolejne rządy. Przykładowo, wskazuje on w odniesieniu do strategii z 2014 roku, że

> „[w]ielokrotne podkreślenie wagi cyberbezpieczeństwa nie pociągało za sobą wskazania konkretnych środków dla podniesienia jego poziomu. Ogólnikowo wskazano na rozwiązania przyczyniające się do rozwoju zdolności do działań defensywnych i ofensywnych, wśród których wskazano m.in. na potrzebę prowadzenia działań o charakterze prewencyjnym i profilaktycznym, wypracowanie i stosowanie właściwych procedur komunikacyjnych czy rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni oraz zapobieganie im[313]. Stopień ogólności wskazanych »rozwiązań« nie sprawia wrażenia jakoby wykonanie tych założeń, miało być w jakikolwiek sposób weryfikowalne." (s. 87).

Kolejna strategia omawiana jest podobnym tonem:

> „Kolejnym dokumentem, który należy przywołać i omówić jest Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022[317]. Dokument ten nie może być postrzegany jako przełomowy lub poruszający nowe istotne kwestie w kontekście wcześniej omawianych opracowań. Już jego twórcy nie pozostawiają w tym zakresie złudzeń, podkreślając na wstępie, że strategia ta stanowi kontynuację działań przyjętych w ramach Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 r.318, przy czym kontynuacja powinna być rozumiana jako odłożenie tych zadań na kolejny okres." (s. 88-89).

Uzasadnioną i odważną krytykę działań władzy uznaję za pozytywny aspekt rozprawy. Ponadto podrozdział ten relatywnie wiernie odzwierciedla stan wdrożenia norm dotyczących cyberbezpieczeństwa na poszczególnych etapach.

Rozdział III „Dyrektywa NIS i Ustawa o krajowym systemie cyberbezpieczeństwa" w sposób centralny dotyczy pytania postawionego we wstępie, omawia on bowiem dwa podstawowe akty prawne stanowiące o obowiązkach dostawców usług cyfrowych. Rozdział wprowadza czytelnika zarówno w społeczne aspekty stanowiące o celowości wprowadzenia dyrektywy NIS oraz w prace nad samą dyrektywą, zarówno koncepcyjne, jak i w toku procesu legislacyjnego. Szczegółowe omówienie wywodu zawartego w tym rozdziale przekracza format niniejszej recenzji, jednakże zauważyć należy, że wywód daje klarowny i poukładany obraz przyczyn istnienia określonych norm dyrektywy NIS, a także implementującej ją ustawy.

Rozdział IV „Dostawcy usług cyfrowych w krajowym systemie cyberbezpieczeństwa" przedstawia szczegółowo u.k.s.c. omawiając system instytucjonalny oraz szczegółowe obowiązki i uprawnienia dostawców usług cyfrowych. Habilitant w ramach tego rozdziału proponuje rozwiązanie szeregu wątpliwości interpretacyjnych na gruncie ustawy. Słusznie zauważa, że pomimo zamkniętego katalogu podmiotów k.s.c. nazwy poszczególnych kategorii mają charakter nieostry. Ciekawą propozycją jest także interpretacja terminu „najnowszy stan wiedzy", z której wynika tożsamość z terminem „stan techniki" w rozumieniu art. 25 ust. 1 p.w.p.

Rozdział V „Spełnianie obowiązków i wymagań nałożonych na dostawców usług cyfrowych" już w tytule nawiązuje do zaproponowanego przez Habilitanta podziału na obowiązki i wymagania względem dostawców usług cyfrowych. Rozdział koncentruje się wokół na identyfikacji tych obowiązków oraz zaproponowaniu mechanizmów umożliwiających ich spełnienie. Cennym elementem rozdziału jest omówienie norm z rodziny ISO/IEC 27000, które pozwala na przypisanie ogólnych norm u.k.s.c. do bardziej szczegółowo określonych, ale jeszcze nie skonkretyzowanych, obowiązków w zakresie zarządzania bezpie-

czeństwem informacji. W rozdziale omówiono także wytyczne ENISA, zarówno w zakresie treści poszczególnych dokumentów, jak i ich charakteru.

Zakończenie, stosunkowo obszerne, stanowi podsumowanie wniosków poszczególnych rozdziałów oraz ocenę omawianych aktów normatywnych i postulaty *de lege ferenda*. Istotnie pozytywnym aspektem pracy jest fakt, że proponowane postulaty zostały już częściowo uwzględnione w dyrektywie NIS2 (rozszerzenie katalogu podmiotów objętych obowiązkami). Niestety, zakończenie ujawnia pewien błąd warsztatowy polegający na nieodniesieniu się wprost do postawionej we wstępie hipotezy. Nie jest to błąd krytyczny, ponieważ czytelnik może doszukać się we wnioskach tych, które stanowią wynik badania prawdziwości postawionej hipotezy; uważam jednak, że praca tego typu powinna zawierać wprost rozstrzygać o prawdziwości swej jedynej hipotezy.

Pomimo pewnych zastrzeżeń metodologicznych i warsztatowych, głębia wywodu oraz jego pionierski zakres pozwalają na uznanie, że monografia spełnia wymóg, o którym mowa w art. 219 ust. 1 pkt 2 p.s.w.n.

1.2. Wydawnictwo

Przepis art. 221 ust. 8 p.s.w.n. nakłada na recenzenta także obowiązek oceny tego, czy monografia została wydana 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 p.s.w.n. Przedmiotowa monografia została oznaczona jako wydana przez Instytut Wydawniczy EuroPrawo. Wykaz sporządzony na podstawie art. 267 ust. 2 pkt 2 lit. a p.s.w.n. został opublikowany w Biuletynie Informacji Publicznej MEiN w drodze Komunikatu Ministra Nauki i Szkolnictwa Wyższego z dnia 29 września 2020 r. w sprawie wykazu wydawnictw publikujących recenzowane monografie naukowe, co odpowiada wymogom art. 267 ust. 3, zgodnie z którym wykaz sporządza minister i udostępnia w BIP na swojej stronie podmiotowej. W wykazie pod pozycją 274 w rubryce Poziom I ujęto Instytut Wydawniczy EuroPrawo, zatem bez wątpliwości przedsta-

wiona monografia została opublikowana sposób czyniący zadość wymogowi przepisu art. 219 ust. 1 pkt 1 lit. a p.s.w.n.

2. Pozostałe osiągnięcia naukowe

Obok wskazanej powyżej monografii wniosek obejmuje 30 innych pozycji. Pozycje te mają zróżnicowany poziom, co wydaje się naturalne – wszakże z wiekiem zmienia się warsztat naukowca. Szkoda, że wiele z tych publikacji przemilcza kwestię stawianych hipotez, pytań badawczych i stosowanych metod. W większości publikacje świadczą o bardzo dobrej znajomości problematyki prawa nowych technologii przez Habilitanta.

2.1. 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.

Artykuł analizuje zmiany wprowadzone dyrektywą NIS2 (w odniesieniu do dyrektywy NIS) w kontekście jej potencjalnego wypływu na rynek pracy w obszarze cyberbezpieczeństwa. Postawione pytanie badawcze jest ciekawe i istotne. Artykuł posługuje się poprawną metodyką oraz wysnuwa wyraźną konkluzję w odniesieniu do postawionego pytania o wpływ NIS2 na rynek pracy. Dodatkowym atutem jest także uporządkowanie doktrynalne zmian w zakresie podmiotów obowiązanych z NIS2. Artykuł ten zaliczam do prac, o których mowa w art. 219 ust. 1 pkt 2 p.s.w.n.

2.2. J. Piecha, M. Porzeżyńska, M. Porzeżyński, M. Grzywacz, Road to Eco-Routing: A Model of Regulatory Approach for the EU, Studia Iuridica 2022, t. 95.

Artykuł dotyczy możliwości wprowadzenia na gruncie prawa UE eco-routingu. Praca ma charakter interdyscyplinarny i obejmuje propozycję norm nakazujących wyposażenie wszystkich systemów nawigacyjnych w tryb eco-routingu jako ustawienia domyślnego. Propozycja ta wydaje się jednak niewystarczająco przemyślana, mogłaby bowiem znacząco utrudnić konkurowanie przez mniejszych twórców nawigacji (np. twórców open-source) uprzywilejowując tym samym dużych graczy takich jak Google Maps.

2.3. M. Porzeżyński, Prawne i etyczne ograniczenia wykorzystania danych biometrycznych w Unii Europejskiej i Polsce, Studia Iuiridica 2022, t. 94.

Artykuł analizuje prawne i etyczne ograniczenia wykorzystania danych biometrycznych w Unii Europejskiej i Polsce w kontekście dynamicznego rozwoju technologicznego. Artykuł konkluduje, że ograniczenia prawne, w szczególności wymóg przeprowadzenia oceny skutków dla ochrony danych (DPIA) oraz zasada minimalizacji danych, stanowią obecnie najważniejszy mechanizm ochrony praw jednostki. Artykuł ten zaliczam do prac, o których mowa w art. 219 ust. 1 pkt 2 p.s.w.n.

2.4. M. Porzeżyński, Problematyka własności danych generowanych w ramach Internetu rzeczy, Państwo i Prawo 2021, nr 2

Artykuł analizuje problematykę „własności" danych generowanych przez urządzenia Internetu rzeczy (IoT), wskazując na zasadniczą lukę w obowiązujących regulacjach prawnych. Autor wykazuje, że żaden z obowiązujących reżimów prawnych nie zapewnia kompleksowej ochrony interesów podmiotów ponoszących nakłady finansowe i organizacyjne związane z gromadzeniem danych IoT, co stanowi barierę dla rozwoju gospodarki opartej na danych. W konkluzji postuluje potrzebę stworzenia nowego rozwiązania prawnego. Wartościowym aspektem artykułu jest względnie szczegółowy opis rzeczywistego problemu wynikłego na gruncie danych pozyskiwanych z IoT. Słabą jego stroną jest niewystarczający aparat dogmatyczny użyty do opisu praw, które miałyby względem tych danych przysługiwać.

2.5. M. Porzeżyński, Glosa do wyroku Sądu Najwyższego z dnia 13 lutego 2019 r. o sygn. akt III PK 13/18 – częściowo krytyczna, Przegląd Prawniczy Uniwersytetu Warszawskiego 2020, nr 2.

Artykuł stanowi glosę częściowo krytyczną do wyroku dotyczącego zwolnienia pracownika za użycie prywatnego pendrive'a w komputerze służbowym. Sądy niższych instancji uznały, że choć użycie pendrive'a stanowiło naruszenie procedur, brak dowodów na skopiowanie danych uniemożliwia uznanie tego za ciężkie naruszenie obowiązków pracowniczych uprawniające do rozwiązania umowy bez wypowiedzenia. Autor polemizuje z tym stanowiskiem, argumentując, że samo podłączenie nieautoryzowanego nośnika stwa-

rza istotne zagrożenie dla bezpieczeństwa organizacji poprzez możliwość infekcji złośliwym oprogramowaniem lub wycieku danych. Wydaje się, że pogląd wyrażony w tekście stanowi obecnie przeważający pogląd na ocenę podobnych stanów faktycznych. Artykuł ten zaliczam do prac, o których mowa w art. 219 ust. 1 pkt 2 p.s.w.n.

2.6. M. Porzeżyński, Ochrona danych osobowych w procesie badania dokumentacji spółki, Palestra 2019, nr 3.

Artykuł podejmuje istotną i dotąd niewystarczająco zbadaną problematykę ochrony danych osobowych w procesie badania dokumentacji spółki w kontekście wymogów RODO. Autor zasadnie identyfikuje lukę w literaturze przedmiotu. Wartością pracy jest próba uporządkowania praktyk rynkowych.

2.7. M. Porzeżyński, Twórczość i autorstwo w dobie sztucznej inteligencji. Wyzwania stojące przed prawem własności intelektualnej, Themis Polska Nova 2018, nr 3.

Artykuł analizuje wyzwania, jakie rozwój sztucznej inteligencji stawia przed prawem własności intelektualnej, koncentrując się na kwestii autorstwa dzieł generowanych przez programy komputerowe. Autor przedstawia szeroki kontekst technologiczny. Główna teza opiera się na stwierdzeniu, że obowiązujące regulacje przewidują autorstwo wyłącznie dla osób fizycznych, co czyni je nieadekwatnymi wobec twórczości AI. Artykuł ten zaliczam do prac, o których mowa w art. 219 ust. 1 pkt 2 p.s.w.n.

2.8. M. Porzeżyński, Problematyka rozprzestrzeniania nieprawdziwych informacji jako zagadnienia społecznego i prawnego, HORYZONTY BEZPIECZEŃSTWA 2018, nr 11.

Artykuł podejmuje problematykę rozprzestrzeniania nieprawdziwych informacji w Internecie, koncentrując się na mechanizmach ich dystrybucji oraz konsekwencjach społecznych i prawnych. Artykuł charakteryzuje się istotnymi słabościami metodologicznymi. Brakuje wyraźnie sformułowanej hipotezy badawczej, pytań badawczych oraz systematycznego opisu zastosowanych metod.

2.9. M. Porzeżyński, Odpowiedzialność za umieszczenie odesłań w Internecie w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej, Themis Polska Nova 2017, nr 2.

Artykuł stanowi komentarz do orzecznictwa TSUE dotyczącego odpowiedzialności za umieszczanie hiperłączy prowadzących do materiałów chronionych prawem autorskim. Autor koncentruje się na analizie art. 3 ust. 1 dyrektywy 2001/29/WE i ewolucji interpretacji pojęcia "publicznego udostępniania" w kontekście technologii internetowych. Szczególną uwagę poświęca się wyrokom w sprawach Svensson, GS Media, Filmspeler i Pirate Bay.

2.10. M. Porzeżyński, Użycie linków a naruszenie praw własności intelektualnej w świetle orzecznictwa Trybunału Sprawiedliwości UE, kwartalnik naukowy Kultura Popularna 2015, nr 1.

Artykuł problematykę prawną użycia linków internetowych w kontekście naruszenia praw własności intelektualnej. Autor prezentuje analizę dogmatyczno-prawną orzecznictwa unijnego, wyjaśniając techniczne typy linków oraz ich implikacje prawne w świetle Dyrektywy 2001/29/WE. Głównym mankamentem jest brak wyraźnie sformułowanej hipotezy, pytań badawczych, co osłabia wartość naukową publikacji.

2.11. M. Porzeżyński, Implementacja Dyrektywy 2010/13/UE w zakresie product placement w polskim porządku prawnym, Kortowski Przegląd Prawniczy 2015.

Artykuł analizuje proces implementacji Dyrektywy 2010/13/UE dotyczącej lokowania produktu (*product placement*) w polskim prawie. Autorzy przedstawiają ewolucję regulacji unijnych, podkreślając, że dyrektywa pozostawia państwom członkowskim swobodę w zakresie dozwolenia lub zakazu tej praktyki.

2.12. M. Porzeżyński, Wyczerpanie prawa do kopii programu komputerowego w kontekście wyroku C-128/11 UsedSoft GmbH v. Oracle International Corp., Zeszyt Studencki Kół Naukowych Wydziału Prawa i Administracji UAM 2013, nr 3.

Artykuł stanowi relację z treści wyroku TSUE w sprawie UsedSoft v. Oracle dotyczącego wyczerpania prawa do programów komputerowych dystrybuowanych elektronicznie.

2.13. M. Porzeżyński, Uwarunkowania prawne dotyczące ochrony znaków towarowych użytych w reklamie za pomocą odniesień w Internecie, Przegląd Prawniczy Uniwersytetu Warszawskiego 2013, nr 1-2.

Praca omawia ewolucję orzecznictwa europejskiego i polskiego w zakresie dopuszczalności używania cudzych znaków towarowych jako słów kluczowych w wyszukiwarkach internetowych.

2.14. M. Porzeżyńska, M. Porzeżyński, The Future of Consumer Protection and Regulation on Energy Market, w: Routledge Handbook of Consumer Protection in Energy Markets" red. T. Hunter, M. Kraśniewski, M. Czarnecka, J. Malinauskaite, Routledge, Londyn 2024.

Tekst podejmuje próbę nakreślenia przyszłości ochrony konsumentów na rynku energii w kontekście transformacji energetycznej. Autorzy zauważają sprzeczność między naturą prawa konsumerskiego, które ma na celu ułatwienie konsumpcji i ochronę indywidualnych interesów konsumentów, a celami polityki energetyczno-klimatycznej, dążącej do ograniczenia zużycia energii i redukcji emisji.

2.15. M. Porzeżyński, Balansowanie pomiędzy sensem a użytecznością. O problematycznej definicji danych biometrycznych w Unii Europejskiej i Polsce, w: A. Zalcewicz, R. Kędziora (red. nauk.), Nowe technologie. Wartości, prawa, zasady. Księga jubileuszowa z okazji 15-lecia Wydziału Administracji i Nauk Społecznych Politechniki Warszawskiej, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2023.

Artykuł analizuje problematyczną konstrukcję definicji danych biometrycznych w rozumieniu RODO i polskiego prawa. Autor prezentuje kontekst rozwoju technologii biometrycznych, wskazując na dynamikę rynku i potrzebę odpowiednich regulacji prawnych.

2.16. M. Porzeżyński, O potrzebie regulacji w zakresie wykorzystania zdobyczy nowych technologii na przykładzie pojazdów autonomicznych, w: A. Zawidzka-Łojek, D. Bach-Golecka (red.), In veriete concordia. Wyzwania prawa europejskiego, Instytut Wydawniczy EuroPrawo, Warszawa, 2020.

Artykuł stanowi krytyczną analizę polskiej regulacji dotyczącej pojazdów autonomicznych z 2018 r. Wartością pracy jest połączenie analizy dogmatycznej z empirycznym badaniem skutków regulacji oraz element komparatystyczny badań.

2.17. M. Porzeżyński, Valuation of data – the gold of the 21st century, in: M. Jankowska, M. Pawełczyk, S. Augustyn, M. Panfil (eds.), Proving the worth. Putting a value on intellectual property, Difin, Warsaw 2019).

Artykuł podejmuje problematykę wyceny danych jako kluczowego zasobu gospodarki opartej na wiedzy. Autor omawia metody wyceny aktywów niematerialnych (podejście rynkowe, kosztowe oraz dochodowe), a następnie proponuje zastosowanie metody mieszanej uwzględniającej zmienne takie jak źródło danych, ich wiek, dokładność czy możliwość dalszego wykorzystania.

2.18. 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.

Artykuł analizuje wpływ ustawy o krajowym systemie cyberbezpieczeństwa na organizację zarządzania bezpieczeństwem informacji w Polsce. Autor koncentruje się na obowiązkach nałożonych na operatorów usług kluczowych i dostawców usług cyfrowych.

2.19. M. Porzeżyński, Wpływ regulacji prawnych a rozwój rynku e-commerce. Wybrane zagadnienia, w: K. Gutbier, K. Szewczyk, A. Borcuch (red.), Instytucje i prawo. Wyzwania ekonomiczne XXI wieku, Laboratorium Wiedzy Artur Borcuch, Kielce 2019.

Artykuł podejmuje problematykę wpływu regulacji prawnych na rozwój rynku e-commerce w Polsce. Autor zauważa, że nowe regulacje w branży technologicznej są często postrzegane negatywnie jako dodatkowe obciążenia biurokratyczne i przeszkody dla przedsiębiorców, a następnie przedstawia swoje – przeciwne stanowisko.

2.20. M. Porzeżyński, Obowiązek określenia wymagań i potrzeb klienta w świetle ograniczeń wynikających z ogólnego rozporządzenia o ochronie danych osobowych (RODO), w: J. Pokrzywniak (red.), Nowe zasady dystrybucji ubezpieczeń, Wolters Kluwer, Warszawa 2018.

Artykuł podejmuje problem na styku prawa ubezpieczeniowego i ochrony danych osobowych, analizując pozorną kolizję między wymogiem określania wymagań klientów przez dystrybutorów ubezpieczeń a zasadą minimalizacji danych w RODO. Opracowanie ma charakter przede wszystkim opisowy, przedstawiając szczegółowo zasady ochrony da-

nych osobowych, status prawny różnych kategorii dystrybutorów jako podmiotów obowiązanych z RODO.

2.21. M. Porzeżyński, Wykorzystanie ochrony własności intelektualnej organizacji sportowej dla zabezpieczenia źródeł dochodu na przykładzie CrossFit'u, w: A. Ciołek, J. Wnorowski (red.) Prawo. Sport. Finanse. Pomiędzy integralnością autonomicznych regulacji w sporcie a przepisami prawa powszechnie obowiązującego, Wydział Prawa i Administracji Uniwersytetu Warszawskiego, Warszawa 2018.

Artykuł opisuje problematykę ochrony IP na przykładzie CrossFit, na tle Pilates.

2.22. M. Porzeżyński, Rewolucja w podejściu do ochrony danych osobowych w kontekście wejścia w życie RODO, Wyzwania naukowe. Ekonomiczne i prawne wyzwania roku 2018, ISSN 2411-3506, Lwów 2018.

Tekst stanowi zwięzłe wprowadzenie do problematyki RODO.

2.23. M. Porzeżyński, Ograniczenie zasady dostępu do informacji publicznej ze względu na ochronę tajemnicy przedsiębiorcy, w: W. Kitler, J. Taczkowska-Olszewska (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Towarzystwo Wiedzy Obronnej, Warszawa 2017.

Artykuł stanowi przegląd problematyki kolizji prawa do informacji publicznej z ochroną tajemnicy przedsiębiorcy w kontekście ustawy o dostępie do informacji publicznej.

2.24. M. Porzeżyński, Praktyczne aspekty nowelizacji prawa prasowego w zakresie modeli reakcji na artykuł prasowy, w: J. Nowakowska-Grunt, J. Kabus (red.), Badania naukowe świetle uwarunkowań turbulentnego otoczenia, Wydawnictwo Naukowe Sophia, Katowice 2017.

Artykuł stanowi opis nowelizacji prawa prasowego z 2012 roku, koncentrując się problematyce reakcji na artykuły prasowe.

2.25. M. Porzeżyński, Konstrukcje prawne w zakresie oprogramowania o otwartym kodzie, Badania i Rozwój Młodych Naukowców w Polsce, Prawo cz. II, 2017

Artykuł opisuje zagadnienie oprogramowania otwartoźródłowego i jego miejsca w polskim systemie prawnym. Koncentruje się na analizie możliwych konstrukcji prawnych leżących u podstaw dystrybucji tego typu programów komputerowych. W opinii Au-

tora „programy komputerowe rozpowszechniane na podstawie licencji otwartego lub wolnego oprogramowania są bardzo ważnym elementem obecnego świata, jednakże nie mogą one zastąpić programów komputerowych, określanych mianem »własnościowych«".

2.26. M. Porzeżyński, Ochrona konkurencji a ochrona praw własności intelektualnej. Zakaz sprzedaży wiązanej na rynku nowych technologii" Badania i Rozwój Młodych Naukowców w Polsce, Prawo cz. II, 2017

Rozdział poświęcony jest problematyce sprzedaży wiązanej na rynku nowych technologii w kontekście ochrony konkurencji i praw własności intelektualnej. Tekst relacjonuje orzecznictwo dotyczące badanego zagadnienia.

2.27. M. Porzeżyński, Wybrane zagadnienia własności intelektualnej jako czynnika ograniczającego swobodę działalności gospodarczej, w: J. Kostrubiec, P. Szczęśniak, M. Zdyb (red.), Prawno-administracyjne ograniczenia podejmowania i prowadzenia działalności gospodarczej. Materiały konferencyjne (Lublin, 15-16.03.2013 r.), Studenckie Zeszyty Naukowe UMCS, Lublin 2013.

Tekst opisuje wybrane prawa własności intelektualnej, rozpatrując je jako czynnik ograniczenia lub promowania wartości, jaką jest konkurencja.

2.28. M. Porzeżyński, Uwarunkowania dotyczące Jednolitego Patentu Europejskiego oraz możliwe skutki dla Polski wynikające z jego wdrożenia, w: K. Dobosz, M. Scheibe, K. Nowak (red.), In short but to the point – Comments on EU Law, Kraków 2013.

Artykuł stanowi omówienie zagadnień związanych z wprowadzeniem Jednolitego Patentu Europejskiego.

2.29. M. Porzeżyński, Wymagania dotyczące nazw produktów leczniczych oraz ich ochrona (inny tytuł: Wymagania dotyczące nazw produktów leczniczych oraz możliwości ich rejestracji w charakterze znaku towarowego), w: A. M. Bielecki, B. Sasin (red.), Współczesne wyzwania prawa ochrony zdrowia, Koło Naukowe Wydziału Prawa i Administracji Uniwersytetu Warszawskiego Ius et Medicina. Warszawa 2013.

Artykuł stanowi przegląd regulacji dotyczących nazw produktów leczniczych. Autor omawia wymogi wynikające z prawa farmaceutycznego, wytyczne URPL i European Medicines Agency oraz przepisy dotyczące znaków towarowych.

2.30. M. Porzeżyński, Zdolność patentowa programów komputerowych, CH Beck, Warszawa 2017.

Monografia stanowi publikację rozprawy doktorskiej Habilitanta. Praca ta była już przedmiotem oceny w innym postępowaniu. Wydanie w formie monografii ma dwie zasadnicze wady: brak wyraźnie sformułowanych hipotez oraz brak syntezy wniosków w postaci zakończenia. Rodzi to konieczność domyślania się przez czytelnika, jakie są pytania badawcze stawiane przez Autora oraz samodzielnego zebrania porozrzucanych w pracy wniosków. Pomimo tych wad monografia wykazuje wysoki poziom wiedzy w przedmiocie prawa własności intelektualnej oraz stanowi istotny głos w toczonej od dziesięciolegi dyskusji na temat zdolności patentowej oprogramowania.

3. Konkluzja

Mając na uwadze powyższe, stwierdzam, że Habilitant posiada w dorobku osiągnięcia naukowe, stanowiące znaczny wkład w rozwój dyscypliny nauki prawne, a tym samym **osiągnięcia naukowe dra Marka Porzeżyńskiego odpowiadają wymaganiom określonym w art. 219 ust. 1 pkt 2 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce** (t.j. Dz. U. z 2021 r. poz. 478 ze zm.).

Jakub J. Szczerbowski

Podpisano przez/ Signed by:
JAKUB
SZCZERBOWSKI
Data/ Date: 17.10.2025 11:06
mSzafir