Dr hab. Anna Konert, prof. UŁa

Katedra Prawa i Postępowania Cywilnego

Uczelnia Łazarskiego w Warszawie

Warszawa, 08.09.2023 r.

Ocena

dorobku naukowego dr. Marcina Rojszczaka sporządzona w postępowaniu o nadanie stopnia doktora habilitowanego

I. Uwagi ogólne

Recenzja została sporządzona z uwzględnieniem przepisów dotyczących warunków ubiegania się o uzyskanie stopnia doktora habilitowanego. Jak stanowi art. 179 ust. 6 *in principio* p.w.p.s.w.n. *postępowania w sprawie nadania stopnia doktora, stopnia doktora habilitowanego i tytułu profesora wszczęte po dniu 30 września 2019 r. prowadzi się na podstawie przepisów ustawy, o której mowa w art. 1.* Oznacza to, że wnioski składane od dnia 1 października 2019 r. w sprawie nadania stopnia doktora habilitowanego procedowane są wyłącznie w oparciu o przepisy p.s.w.n.

Warunki nadania stopnia doktora habilitowanego zostały unormowane w art. 219 p.s.w.n. Zgodnie z tym przepisem 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.*

Recenzent powołany w postępowaniu habilitacyjnym dr. Marcina Rojszczaka powinien zatem ocenić, czy Kandydat spełnia powyższe warunki.

Stopień doktora nauk prawnych został nadany Panu Marcinowi Rojszczakowi przez Radę Instytutu Nauk Prawno-Administracyjnych Wydziału Prawa i Administracji Uniwersytetu Warszawskiego w dniu 8 października 2018 r. Rozprawa doktorska nosiła tytuł: *Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*. Promotorem rozprawy był dr hab. Cezary Banasiński, prof. UW.

II. Ocena osiągnięć naukowych uzyskanych po otrzymaniu stopnia doktora nauk prawnych, wskazanych przez Habilitanta jako znaczny wkład w rozwój dyscypliny „nauki prawne" zgodnie z art. 219 p.s.w.n. § 2b

1. Wybór problematyki badawczej

W Autoreferacie do osiągnięć naukowych uzyskanych po otrzymaniu stopnia doktora stanowiących znaczny wkład w rozwój dyscypliny „nauki prawne" Habilitant wskazuje na:

Cykl publikacji pt. *„Standardy prawne stosowania nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej"*

Badania prezentowane są w pięciu obszarach merytorycznych, których efekty zostały opublikowane w **dziewiętnastu publikacjach naukowych (łącznie 437 stron),** wydanych w formie artykułów naukowych w latach 2018-2023 w czasopismach, 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 ustawy – Prawo o szkolnictwie wyższym i nauce.

Tematyka poruszona przez Habilitanta jest niezwykle ważna, ale też obszerna, wielowymiarowa i podlegająca licznym aktualizacjom. Problematyka jest szczególnie istotna z punktu widzenia prawa polskiego, zwłaszcza w ramach trwającej debaty dotyczącej zgodności polskich przepisów inwigilacyjnych ze standardami konstytucyjnym (określonym przez Trybunał Konstytucyjny), oraz międzynarodowym i unijnym (określonymi w orzecznictwie Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej).

2. Struktura rozważań

Na cykle publikacji składają się:

. 1) *Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji*, „Państwo i Prawo" 2018/10.

. 2) *UK Electronic Surveillance Programmes in the Context of Protection of EU Citizens' Rights after Brexit*, "Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2018,

. 3) *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, "Ius Novum" 2019/1,

. 4) *Prawne dylematy regulacji cyberprzestrzeni: konflikt pomiędzy bezpieczeństwem narodowym a prawem do prywatności z perspektywy prawodawstwa UE i USA*, "Teka Komisji Politologii i Stosunków Międzynarodowych" 2018/3 (data publikacji lipiec 2019).

. 5) *The ECTHR's Judgment in Case of Centrum för Rättvisa v. Sweden as a Leading Case for the Review of Domestic Regulations on Signals Surveillance*, "Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2019.

. 6) *Does Global Scope Guarantee Effectiveness? Searching for a New Legal Standard for Privacy Protection in Cyberspace*, "Information & Communications Technology Law" 2020/1, DOI: 10.1080/13600834.2020.1705033.

. 7) *Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa*

autorytarnego, „Studia nad Autorytaryzmem i Totalitaryzmem" 2020/2.

. 8) *CLOUD Act Agreements from an EU Perspective*, "Computer Law & Security Review" 2020/09, DOI: 10.1016/j.clsr.2020.105442.

. 9) *Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland*, "Democracy and Security" 2021/1, DOI: 10.1080/17419166.2020.1841367.

. 10) *Compliance of Automatic Tax Fraud Detection Systems with the Right to Privacy Standards Based on the Polish Experience of the STIR System*, "Intertax" 2021/1.

. 11) *Extraterritorial Bulk Surveillance after the German BND Act Judgment*, "European Constitutional Law Review" 2021/1, DOI: 10.1017/S1574019621000055.

. 12) *The uncertain future of data retention laws in the EU: Is a legislative reset possible?*, "Computer Law & Security Review" 2021/7, DOI: 10.1016/j.clsr.2021.105572.

. 13) *Polskie przepisy inwigilacyjne w świetle najnowszego orzecznictwa Trybunału Sprawiedliwości – wnioski krytyczne po wyroku Trybunału Sprawiedliwości z 2.03.2021 r., C-746/18, Postępowanie karne przeciwko H.K.*, „Europejski Przegląd Sądowy" 2021/11.

. 14) *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, "European Constitutional Law Review" 2021/4, DOI: 10.1017/S1574019621000353.

. 15) *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses*, "European Journal of Crime, Criminal Law

and Criminal Justice" 2021/12, DOI: 10.1163/15718174-bja10027.

. 16) *Kontrola sądów krajowych nad stosowaniem środków inwigilacji elektronicznej na tle orzecznictwa ETPC*, „Państwo i Prawo" 2022/4.

. 17) *e-Evidence Cooperation in Criminal Matters from an EU Perspective*, "Modern Law Review" 2022/4, DOI: 10.1111/1468-2230.12749.

. *18) Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa ETPC,* „ Studia Prawa Publicznego" 2022/4, DOI: 10.14746/spp.2022.4.40.6.

. 19) *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna*, „Państwo i Prawo" 2023/2.

W piśmiennictwie naukowym podkreśla się, iż pewna liczba publikacji zostanie uznana za cykl dopiero z perspektywy *ex post*, co w praktyce może oznaczać, "iż autor będzie wydawał publikacje na określony temat, który ze względu na postępujące zmiany ustawowe, kontrowersje w piśmiennictwie bądź orzecznictwo dopiero pozwoli na wskazanie cyklu" (K. Ślebzak, *Jednotematyczny cykl publikacji jako przesłanka nadawania stopnia doktora habilitowanego nauk prawnych*, Państwo i Prawo 2013/7,, s. 35, a także iż „istnienie cyklu zakłada, co do zasady, świadomość jego tworzenia;" (tamże, s. 39).

Artykuły opublikowane w ramach cyklu powinny pozostawać ze sobą w ścisłym związku merytorycznym. Nie mogą to być przypadkowo wybrane publikacje z dorobku. Mają to być po prostu publikacje będące ekwiwalentem monografii. Ta ekwiwalencja powinna ujawniać się w analogicznym nakładzie pracy oraz wpływie na rozwój nauki. Zgodnie z Poradnikiem Rady Doskonałości Naukowej (2021 r.) "...cykl powiązanych tematycznie artykułów

naukowych powinien odpowiadać jeśli chodzi o wartość naukową rozprawie habilitacyjnej w dotychczasowym jej rozumieniu. **Ponadto, potwierdzenie istnienia cyklu jest możliwe, gdy poszczególne publikacje, zebrane w jedną całość, wskazują na oryginalne rozwiązanie problemu naukowego, wnosząc znaczy wkład w rozwój określonej dyscypliny naukowej.** Oznacza to, że wykazanie istnienia cyklu w postępowaniu w sprawie nadania stopnia doktora habilitowanego nie powinno sprowadzać się do podjęcia przez recenzenta pracy koncepcyjnej. Istnienie cyklu zakłada co do zasady świadomość jego tworzenia, podobnie jak w odniesieniu do rozprawy doktorskiej czy uprzednio habilitacyjnej, również od powiązanego tematycznie cyklu publikacji należałoby oczekiwać, że jest on aktualny i uwzględnia stan wiedzy na dzień rozpoczęcia postępowania."[1]

3. Cel, tezy, metody badawcze, zakres badań oraz ocena treści rozważań

Habilitant prowadzi badania w zakresie europejskich standardów stanowionych w obszarze inwigilacji elektronicznej dokonując szczegółowego podziału na pięć obszarów:

1) Państwo demokratyczne a inwigilacja nieukierunkowana;

2) Europejski (unijny) standard zabezpieczeń prawnych;

3) Inwigilacja elektroniczna jako zagrożenie dla standardów państwa prawa – perspektywa krajowa;

4) Doświadczenia innych państw;

5) Inwigilacja elektroniczna w kontekście współpracy transgranicznej.

[1] „Postępowania dotyczące nadawania stopnia doktora habilitowanego", s. 14.

Ani w autoreferacie ani w poszczególnych publikacjach nie zostały wskazane metody badawcze. Niemniej jednak przypuszczalnie w każdej z publikacji została wykorzystana metoda prawno-dogmatyczna. W niektórych także metoda prawno-porównawcza. Ponadto, Habilitant zbadał statystyki sądów karnych dotyczące żarządzania stosowania kontroli operacyjnej i procesowej, a także proces badania okresowych sprawozdań z dostępu do metadanych pochodzących z łączności elektronicznej.

Habilitant stawia następujące tezy badawcze:

1) Programy nieukierunkowanej inwigilacji są fundamentalnie niezgodne z zasadami funkcjonowania państwa demokratycznego, a ich stosowanie nie jest konieczne dla realizacji żadnego prawnie uzasadnionego celu;

2) Programy inwigilacji ukierunkowanej dzięki rozwojowi techniki i postępującej cyfryzacji pozwalają na gromadzenie bardzo szczegółowych danych na temat jednostki, w istocie kopii jej „cyfrowego życia"; istniejące zabezpieczenia prawne, pochodzące sprzed ery cyfryzacji, są nieadekwatne dla kontroli nowych narzędzi inwigilacyjnych, m.in. takich, które wykorzystują oprogramowanie *malware*;

3) Organy publiczne coraz częściej wdrażają technologie cyfrowe, które bazują na gromadzeniu danych nadmiarowych; dane nadmiarowe to parafrazując słowa Humby'ego paliwo dla inwigilacji; w efekcie wiele z tych nowoczesnych technologii, wykorzystywanych w tak różnych obszarach jak ochrona zdrowia, transport czy podatki, ma oczywisty potencjał inwigilacyjny;

4) Rosnącym zdolnościom inwigilacyjnym państw musi odpowiadać ustanowienie spójnego i ponadnarodowego modelu zabezpieczeń

prawnych, podlegającego skutecznym mechanizmom niezależnego nadzoru, opartego na wspólnym poszanowaniu praw podstawowych jako nieprzekraczalnej bariery dla działalności organów publicznych;

5) Zarówno polski model prawny, jak i krajowa praktyka stosowana w obszarze inwigilacji elektronicznej jest antywzorem dla państw demokratycznych, a w świetle zmian wprowadzanych w ostatnich latach zbliża Polskę do rozwiązań znanych z państw wprost autorytarnych.

Ujęcie też nie budzi wątpliwości i jest komunikatywne, nie pozostawia wątpliwości jaki jest cel poszczególnych obszarów badawczych. Habilitant określił założenia dotyczące sposobu analizy tytułowego zagadnienia oraz prawidłowo przeprowadził tę analizę. Analizy przeprowadzone w poszczególnych publikacjach dokonane w celu udowodnienia również mają istotny walor poznawczy oraz praktyczny. Na podkreślenie zasługuje fakt, iż Habilitant doskonale rozumie problematykę, także od strony technicznej z racji swojego wykształcenia.

W ramach poszczególnych obszarów Habilitant jasno wskazał jakie są cele i przedmiot badań. W pierwszym obszarze pt. Państwo demokratyczne a inwigilacja nieukierunkowana badany był związek pomiędzy stosowaniem nieukierunkowanej inwigilacji a tzw. efektem mrożącym w zakresie prawa do informacji oraz negatywny wpływ tych środków na wolność wyrażania poglądów oraz na stabilność procesu wyborczego. Habilitant dochodzi do wnioksu, iż istnienie tej formy nadzoru przyzwyczaja społeczeństwo do asymetrii informacyjnej, a przez to także do podejmowania przez organy władzy publicznej działań naruszających zasadę konieczności i proporcjonalności. Analizie poddano szereg orzeczeń sądów krajowych oraz ETPC i TSUE.

Drugi obszar badań dotyczący standardów zabezpieczeń prawnych, jakie

powininny być stosowane dla kontroli ryzyk związanych z działalnością inwigilacyjną państwa zawiera analizę licznych orzeczeń ETPC wskazując na ewolucję w poglądach Trybunału oraz badając czy standard ETPC jest wystarczający dla ochrony przed zagrożeniami związanymi z upowszechnianiem nowoczesnych środków inwigilacyjnych. Habilitant ponadto, dokonuje analizy siedmiu orzeczeń TSUE dotyczących stosowania ogólnego obowiązku retencji danych, które uznaje za spójne i podziela stanowisko Trybunału dotyczące niedopuszczalnośćci stosowania uogólnianych form retencji (zarówno w zakresie walki z poważną przestępczością, jak i dla celów bezpieczeństwa narodowego). Kolejnym tematem badań było wykorzystywanie nowoczesnych środków inwigilacji elektronicznej do gromadzenia dowodów na potrzeby trwających postępowań karnych, w którym to Habilitant zgłasza kilka postulatów: zainicjowanie refrormy obowiązujących przepisów, ustanowienie zasad stosowania nowoczesnych form inwigilacji ukierunkowanej jako elementu unijnej współpracy w sprawach karnych oraz wreszcie, wprowadzenie nowych typów zabezpieczeń prawnych (obligatoryjną certyfikację narzędzi inwigilacyjnych oraz mechanizm trwałych logów) tworzących podstawę dla ustanowienia zewnętrznego i niezależnego organu kontrolnego, stojącego na straży legalnego stosowania uprawnień inwigilacyjnych.

Na aprobatę zasługują rozważania, a zwałszcza wynikające z nich wnioski w ramach trzeciego obszaru badań, w którym to Habilitant omawia perspektywę krajową. Wskazuje wpierw, iż polskie przepisy inwigilacyjne od wielu lat były dalekie od europejskich standardów, zwałszcza w zakresie środków stosowanych w obszarze walki z przestępczością. Krytycznie został oceniony blankietowy charakter uprawnień dotyczących inwigilacji elektronicznej stosowanej w obszarze wywiadu krajowego oraz zagranicznego. Habilitant następnie stawia ciekawe pytanie: czy to niedemokratyczne zmiany

doprowadziły do zwiększenia uprawnień inwigilacyjnych, czy też rozbudowane mechanizmy inwigilacyjne stały się przyczyną dalszej erozji demokracji? Wyniki badań zostały przedstawione w publikacjach *„Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland"* [Załącznik nr 3, poz. 9] oraz *„Polskie przepisy inwigilacyjne w świetle najnowszego orzecznictwa Trybunału Sprawiedliwości..."*. Po pierwsze brak jest ustanowienia zabezpieczeń prawnych, które wynikają ze standardów europejskich, a po drugie Habilitant wskazuje na cały zestaw zmian dotyczących rozliczalności działań inwigilacyjnych, w tym czynności prowadzonych w ramach procedury karnej, które istotnie oddziałują na skuteczność ochrony przed ryzykiem nadużycia władzy. Cenny naukowo element tego obszaru to szczegółowa analiza statystyk sądów karnych dotyczących zarządzania stosowania kontroli operacyjneji procesowej oraz przykłady budowania przez organy publiczne dużych baz danych, które następnie wykorzystywane są niezgodnie z pierwotnym przeznaczeniem (w tym zwłaszcza kazus systemu STIR, czy procedura *in vitro*).

Kolejny, czwarty obszar badań zawiera analizę prawno-porówczwczą dotyczącą nieograniczonych form przechwytywania łączności i to stosowanych w obszarze co do zasady wyłączonym z zakresu stosowania prawa UE (obronność/wywiad zagraniczny). Habilitant omawia przepisy inwigilacyjne stosowane w Szwecji, Wielkiej Brytanii, Niemczech oraz Stanach Zjednoczonych. Dokonana przez Habilitanta komparatystyka regulacji tych Państw uwidacznia znaczne różnice w jakości stanowionego prawa.

Wreszcie, ostatni obszar badań dotyczący współpracy ponadnarodowej obejmuje zwłaszcza kwestię współpracy międzynarodowej w zakresie gromadzenia i wymiany dowodów elektronicznych. Habilitant dochodzi do wnisoku, iż ułatwienie transgranicznej wymiany dowodów elektronicznych

będzie naturalnym impulsem dla standaryzacji zasad prowadzenia inwigilacji. Ponadto, zgłasza postulat uzupełnienia rozporządzenia o dowodach elektronicznych nowym aktem prawnym ustanawiającym minimalny zakres zabezpieczeń prawnych, stosowanych w obszarze legalnej inwigilacji prowadzonej w sprawach karnych.

4. Formalna ocena publikacji

Formalna strona poszczególnych publikacji nie budzi większych zastrzeżeń. Publikacje pisane są poprawnym językiem. Przypisy są czytelne. Źródła zostały poprawnie udokumentowane. Literatura poprawnie wykorzystana.

5. Ocena końcowa

W ocenie recenzenta przedstawiony przez Habilitanta cykl 19 publikacji stanowi ekwiwalent monografii (łącznie 437 stron). Ponadto, ocena merytoryczna treści tychże artykuów wypada pozytywnie oraz poszczególne publikacje, zebrane w jedną całość, wskazują na oryginalne rozwiązanie problemu naukowego i wnoszą znaczy wkład w rozwój dyscypliny naukowej.

W konkluzji wskazany więc cykl publikacji pt ***„Standardy prawne stosowania nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej”***, może być uznany za osiągnięcie naukowe stanowiące znaczny wkład w rozwój prawa, o którym mowa w art. 219 p.s.w.n. § 2b.

III. Ocena osiągnięć naukowych zgodnie z art. 219 p.s.w.n. § 3

1. Struktura rozważań

W okresie po uzyskaniu stopnia doktora nauk prawnych w 2018 r. Pan dr Marcin Rojszczak powiększył swoją działalność badawczo-naukową, wskazując w Autoreferacie na 23 publikacje, na które składają się:

- monografia (opublikowana jako rozprawa doktorska),
- rozdziały w monografiach 12,
- artykuły w recenzowanych czasopismach naukowych 10 (w tym 4 we współautorstwie).

Ponadto, Habilitant opublikował 7 artykułów naukowych w okresie poprzedzającym uzyskanie stopnia doktora:

1) *Odpowiedzialność za przetwarzanie danych przez portal społecznościowy – glosa do wyroku TSUE z 5.06.2018 r., C-210/16*, Europejski Przegląd Sądowy 2018/10.

2) *Międzynarodowa współpraca organów podatkowych a dopuszczalny zakres ingerencji w prawa podstawowe – uwagi krytyczne po dwóch latach obowiązywania umowy FATCA*, Przegląd Prawa Handlowego 2018/8.

3) *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne*, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2018/4.

4) *Skuteczność ochrony praw podmiotów danych wynikających z prawa UE w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA*, Transformacje Prawa Prywatnego 2018/1.

5) *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE*, Prawo Mediów Elektronicznych 2017/3.

6) *Ochrona tajemnicy adwokackiej, a usługi świadczone w chmurze obliczeniowej*, Studia Prawnicze (PAN) 2017/2.

7) *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE.*

8) *z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, Studia Prawa Publicznego 2017/2.

2. Ocena dorobku

Brak jest w obowiązujących przepisach prawa legalnej definicji pojęcia „aktywność naukowa", a samo pojęcie to ma charakter nieostry. Według Rady Doskonałości Naukowej pojęcie to należy rozumieć szeroko. Aktywność taka powinna być realizowana w innych określonych podmiotach, nie zaś w podmiocie, w którym zatrudniona jest osoba ubiegająca się o nadanie stopnia doktora habilitowanego. Taka aktywność musi być realizowana w co najmniej dwóch uczelniach, instytucjach naukowych lub instytucjach kultury. Z kolei, sformułowanie „w szczególności zagranicznej" stanowi przesłankę wartościującą aktywność naukową, nie zaś warunek konieczny jej spełnienia.[2]

Oceniając dorobek naukowy Habilitanta, zwłaszcza dorobek publikacyjny, należy zauważyć, iż układa się on w kilka obszarów badawczych.

[2] „Postępowania dotyczące nadawania stopnia doktora habilitowanego", s. 15.

Badania prowadzone były w dwóch ośrodkach badawczych, w Politechnice Warszawskiej, gdzie jest zatrudniony od 2019 r. oraz na Uniwersytecie Gdańskim, gdzie prowadzi działalność dydaktyczną odbywał staż naukowy w Katedrze Prawa Informatycznego WPiA UG w 2022. Współpraca z Katedrą prowadzona była także wcześniej, na co wskazuje Habilitant, czego efektem jest m.in. jego udział w monografii *„Nowe technologie w praktyce prawnika"* (Wydawnictwo Arche, 2021) a także zaproszenie do udziału w organizowanej w 2019 r. przez WPiA UG konferencji „Rok z RODO".

Przede wszystkim, przedmiotem badań dr Rojszczak uczynił zagadnienie cyberbezpieczeństwa, w tym bezpieczeństwa usług prawnych, w tym właśnie promowanie dobrych praktyk w zakresie cyberbezpieczeństwa wśród prawników (stosowanie tzw. zasad cyberhigieny). Zaletą tych rozważań jest rozumienie tej problematyki także z punktu widzenia technicznego, a to dzięki wykształceniu oraz doświadczeniu zawodowemu Habilitanta. Podejmuje on tę problematykę wieloaspektowo, najwięcej uwagi poświecając na dyskusję w zakresie przyszłości unijnego modelu cyberbezpieczeństwa. Ten obszar badań zawiera szereg publikacji, zarówno wydanych na rynku krajowym, jak i zagranicznym. Razem z prof. Banasińskim Habilitant był także współredaktorem monografii *„Cyberbezpieczeństwo"* (Wolters Kluwer, 2020), pierwszej tego typu publikacji wydanej w Polsce podejmującej problematykę cyberbezpieczeństwa w sposób wieloaspektowy. Był również współredaktorem zeszytu Internetowego Kwartalnika Antymonopolowego i Regulacyjnego 2020/2, pt. *„Ochrona konkurencji i konsumentów a unijny model cyberbezpieczeństwa"*. Habilitant zajmuje się również problemem prawnej regulacji cyberbezpieczeństwa produktów kierowanych na rynek konsumencki (np. *„Cybersecurity of Consumer Products against the Background of the EU Model of Cyberspace Protection"*. Jak słusznie zauważa, z uwagi na dynamicznie wzrastającą liczbę tzw. usieciowionych produktów

konsumenckich, a także masową ekspansję rynku IoT coraz częściej zagrożenia dla bezpieczeństwa czy prywatności mają swoje źródła w podatnościach wykorzystanych w powszechnie wykorzystywanych produktach konsumenckich. Kwestia ta w ostatnich latach wywołuje ożywione dyskusje, a zwłaszcza w kontekście odpowiedzialności cywilnej związanej z rozwojem nowych technologii. Na rynek trafia coraz więcej nowych technologii, np. dla inteligentnego domu. Artykuły gospodarstwa domowego, takie jak piekarniki, kamery bezpieczeństwa, ekspresy do kawy mogą być teraz obsługiwane zdalnie ze smartfonów i tabletów. Ponadto coraz częściej mówi się o zjawisku sztucznej inteligencji (AI – *Artificial Intelligence*), Internetu Rzeczy (IoT *Internet of Things*), drukowaniu przestrzennym, robotach, czy też zautomatyzowanych (autonomicznych) pojazdach mechanicznych. W raporcie przygotowanym przez McKinsey Global Institute (MGI) wskazuje się na 12 obszarów techonologii, które mogą mieć ogromny wpływ na życie i pracę ludzi, a także na rozwój gospodarczy. Autorzy raportu starają się również oszacować potencjalny wpływ ekonomiczny każdej z tych technologii na zastosowania w 2025 r.[3] Wśród tych obszarów znalazły się, m.in. zaawansowana robotyka (automatyka) oraz autonomiczne lub częściowo autonomiczne pojazdy. Należy stwierdzić, iż Internet Rzeczy[4] stanowi czwartą rewolucję technologiczną, kiedy to dwa przedmioty są w stanie ze sobą się komunikować. Może się okazać, że szkoda zostanie spowodowana nie z błędu oprogramowania, ani z winy użytkownika, tylko przykładowo na skutek awarii sieci telefonii komórkowej. Zasady odpowiedzialności za produkt nie miałyby zastosowania do operatora sieci (niebędącego producentem, importerem lub sprzedawcą produktu). Często cecha

[3] Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy, Maj 2013 r.:https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx,

[4] Zob. Raport „Internet Rzeczy – Polska Przyszłości" Grupy Roboczej ds. Internetu Rzeczy (Internet of Things - IoT) przy Ministerstwie Cyfryzacji, https://www.gov.pl/web/cyfryzacja/grupa-robocza-ds-internetu-rzeczy-internet-of-things-iot

technologii wywołuje nieznane dotąd problemy w ukształtowaniu przesłanek odpowiedzialności odszkodowawczej, jak np. wymagany standard staranności, czy też zdefiniowanie wady produktu.

Drugim obszarem badawczym są kwestie związane z ochroną danych osobowych oraz prawem do prywatności. Zapewnienie ochrony prywatności oraz ochrony danych osobowych obywateli to ogromne wyzwanie w erze wykorzystywania nowych technologii, w tym technologii *big data,* która pozwala na przeprowadzenie identyfikacji jednostki nawet na podstawie informacji poddanych wcześniejszej anonimizacji, a także ustalenie wrażliwych danych osobowych na podstawie danych publicznie dostępnych. Na szczególne podkreślenie zasługują rozważania Habilitanta przedstawione w artykule *„Definicja i granice prawnej ochrony prywatności w epoce analityki big data* ". Habilitant podejmuje się ważnego zadania przeanalizowania czy podstawy europejskiego modelu ochrony danych w sposób prawidłowy definiują zarówno przedmiot ochrony, jak i sposób jej zapewnienia, w konsekwencji upowszechnienia analiz *big data.* Doskonale argumentuje pogląd, że upowszechnienie analityki *big data* (lub nowych, bardziej zaawansowanych technologii) sprawi, że dalsze funkcjonowanie znanych obecnie prawnych mechanizmów ochrony prywatności stanie się bezcelowe. Pomocna tu była także analiza prawno-porównawcza, której dokonał Habilitant.

Kolejny bardzo cenny naukowo element to analiza relacji technologii *blockchain* do zagadnienia ochrony danych osobowych. Wykorzystanie tej technologii może stanowić źródło dwóch rodzajów trudności związanych z przetwarzaniem danych osobowych. Po pierwsze, problem dotyczy identyfikacji ról zdefiniowanych przez RODO. Kim jest administrator danych osobowych? Czy da się zidentyfikować podmiot przetwarzający dane? Zależnie od odpowiedzi na te pytania różnie będą się rozkładać obowiązki uczestników

sieci *blockchain* oraz ich odpowiedzialność. Po drugie, problem może dotyczyć obowiązku zapewnienia praw osób, których dane są przetwarzane. W szczególności jest to prawo do informacji, kto, w jaki sposób i jak długo przetwarza dane. Jest to także prawo do żądania poprawienia danych lub zaprzestania ich przetwarzania. Trwałość informacji zapisanych w łańcuchu bloków utrudnia, lub wręcz uniemożliwia, wypełnienie wszystkich tych praw. Habilitant dokonuje prawidłowej analizy tej problematyki dochodząc finalnie do wniosku, iż to nie kwestia zgodności z prawem ochrony danych, ale problem zrozumienia źródeł „zaufania" w stosunkach społecznych może okazać się kluczowy dla sukcesu wykorzystania tej technologii.

Wreszcie, ostatnim obszarem badań są prawne aspekty funkcjonowania nowoczesnych systemów algorytmicznych, w tym sztucznej inteligencji. Na rynek trafia coraz więcej nowych technologii na przykład dla inteligentnego domu. Problematyka związana z regulacjami technologii przełomowych stanowi obecnie duże zainteresowanie nauki i zasługuje na aprobatę.

W publikacji "Prawne aspekty...." przeprowadzono dyskusje terminologiczne oraz polemikę z autorami raportu opublikowanego w listopadzie 2018 r. planu działań Ministerstwa Cyfryzacji pt. *Założenia do strategii AI w Polsce*. Habilitant wyjaśnia tu wątpliwości termonologiczne (wskazując m.in. na różnice między ML oraz SI, silną a słabą SI) oraz wskazuje na kierunki ewolucji badań nad sztuczną inteligencją. Na aprobatę zasługują rozważania dotyczące odpowiedzialności za szkody spwodowane przez SI. Sam Habilitant wskazuje, iż właśnie ta kwesia stanowi główną barierę rozwoju rynku SI (s. 6). W 2020 roku instytut badania opinii publicznej IPSOS przeprowadził europejskie badanie przedsiębiorstw dotyczące wykorzystania technologii opartych na sztucznej inteligencji. Odpowiedzialność cywilna znalazła się wśród trzech największych barier w korzystaniu z SI przez przedsiębiorstwa

europejskie. Kwestia ta została również uznana za najistotniejszą zewnętrzną przeszkodę dla firm, które planują w przyszłości wdrożyć systemy sztucznej inteligencji do swojej działalności.

Obecne krajowe przepisy dotyczące odpowiedzialności cywilnej nie są dostosowane do kwestii roszczeń z tytułu odpowiedzialności za szkody spowodowane przez produkty i usługi wspierane przez sztuczną inteligencję. Zgodnie z takimi przepisami, powód w postępowaniu cywilnym o uzyskanie odszkodowania musi udowodnić bezprawne działanie lub zaniechanie osoby, która spowodowała szkodę. W przypadku systemów sztucznej inteligencji jest to znacznie utrudnione. SI cechuje się złożonością, daleko idącą autonomią i nieprzejrzystością (tzw. efekt czarnej skrzynki, polegający na tym, że możliwe jest zobaczenie danych wejściowych i wyjściowych, natomiast brak jest wglądu w same procesy podejmowania decyzji przez SI). W związku z tym zidentyfikowanie osoby odpowiedzialnej za szkodę powstałą w wyniku działania systemu sztucznej inteligencji generuje duże problemy. Habilitant słusznie wskazuje się na zbyt dużą ilość podmiotów i podwykonawców, których ewentualna odpowieizlność mogłaby być brana pod uwagę. Habilitant podważa, słusznie, teorię odpowiedzialności faktycznego dysponenta SI, wskazując, iż zwolnia ona producenta z odpowiedzialności i nie wyjaśnia wielu wątpliwości interpretacyjnych. Prawidłowo też zostały przeanalizowane przepisy europejskie i krajowe dotyczące odpowiedzialności za produkt wadliwy. Polskie przepisy dotyczące odpowiedzialności za produkt zostały wprowadzone do kodeksu cywilnego (art. 449^1–449^{10}) jako skutek implementowania dyrektywy 85/374/EWG, która ukształtowała polskie prawo deliktowe w tym zakresie. Usytuowanie przepisów KC pomiędzy normami o odpowiedzialności deliktowej a regułami określającymi odpowiedzialność wynikającą z niewykonania lub nienależytego wykonania zobowiązania nie było przypadkowe. Ponieważ odpowiedzialność za szkodę wyrządzoną przez produkt niebezpieczny wykazuje

cechy, które niepozwalają zakwalifikować jej jednoznacznie jako odpowiedzialności deliktowej czy kontraktowej, powstał więc nowy reżim pozaumownej odpowiedzialności odszkodowawczej, konstruowanej w oparciu o zasadę ryzyka, występującą zarówno w odpowiedzialności *ex delicto*, jak i *ex contractu.* Habilitant wskazuje, iż ich stosowanie powoduje wiele wątpliwości praktycznych, np. przy stosowaniu momentu "wprowadzenia do obrotu", czy też samej definicji "produktu", która nie jest dostosowana do współczesnego rozwoju SI.

Dyrektywa uchwalona 30 lat temu, a także przepisy wewnetrzne poszczególnych Państw członkowski UE implementujące ją, mogą okazać się niewystarczające by zapewnić ochronę poszkodowanych w dobie rozwoju nowych technologii, wykorzystywania robotów, pojazdów autonomicznych, czy tworzenia smart cities, Internetu rzeczy itd.

W 2018 r. Komisja przygotowała sprawozdanie dla Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego dotyczące stosowania dyrektywy Rady w sprawie zbliżenia przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich dotyczących odpowiedzialności za produkty wadliwe (85/374/EWG)[5], w którym dokonuje oceny skuteczności tejże dyrektywy. W ocenie wzięto pod uwagę najnowsze osiągnięcia technologiczne oraz oceniono czy dyrektywa: zachowuje skuteczność w zakresie realizacji jej pierwotnych celów; jest efektywna; jest spójna zwłaściwymi przepisami UE; zachowuje przydatność dzięki uwzględnieniu najnowszych osiągnięć technologicznych; oraz czy prawodawstwo UE wzakresie odpowiedzialności za produkty nadal zapewnia wartość dodaną przedsiębiorcom i osobom poszkodowanym. [6]

[5] Bruksela, dnia 7.05.2018 r. COM (2018) 246 final.

[6] *Ibidem*, s. 2.

Komisja zwróciła szczególną uwagę na rozwój nowych technologii badając też, czy dyrektywa niepotrzebnie nie zniechęca producentów przed wprowadzeniem do obrotu innowacyjnych produktów? Ocena wykazała, iż w pewnych obszarach dyrektywa pozostawia kilka kwestii wymagających wyjaśnienia, a zwłaszcza w zakresie nowopowstających technologii cyfrowych, autonomicznych i inteligentnych. Pojęcia, które były jasno określone 30 lat temu, kiedy uchwalono dyrektywę., na przykład „produkt" i „producent" lub „wada" i „szkoda", stały się obecnie mniej wyraziste. Konieczna jest pogłębiona analiza wpływu zmian technologicznych (na przykłąd produktów autonomicznych) na odpowiedzialność za produkty. Komisja stworzyła grupę ekspercką ds. odpowiedzialności, która występuje w dwóch konfiguracjach. Pierwsza grupa (przedstawiciele państw członkowskich, przemysłu, organizacji konsumenckich, społeczeństwa obywatelskiego i środowiska akademickiego) ma dokonać interpretacji oraz ewentualnej aktualizacji dyrektywy, w tym w świetle zmian w orzecznictwie europejskim i krajowym, wpływu nowych i nowopowstających technologii oraz wszelkich innych zmian w dziedzinie odpowiedzialności za produkty. Druga grupa (niezależni eksperci akademiccy i praktycy) ma dokonać oceny, czy ogólny system odpowiedzialności jest właściwy dla ułatwienia wdrażania nowych technologii dzięki wspieraniu stabilności inwestycji i zaufania konsumentów.[7]

Może się też okazać, że szkoda zostanie spowodowana nie z błędu oprogramowania, ani z winy użytkowanika, tylko przykładowo na skutek awarii sieci telefonii komórkowej. Zasady odpowiedzialności za produkt nie miałyby zastosowania do operatora sieci (nie będącego producentem, importerem lub sprzedawcą produktu). Często cecha technologii wywołuje nieznane dotąd

[7] *Ibidem*, s.11.

problemy w ukształtowaniu przesłanek odpowiedzialności odszkodowawczej, jak np. wymagany standard staranności, czy też zdefiniowanie wady produktu.[8]

Habilitant wskazuje na alternatywę dla ustanowienia odrębności prawnej osób elektronicznych w postaci wykorzystania do celu zwiększenia bezpieczeństwa obrotu bezpośrednio osoby prawnej. System informatyczny miałby być niejako wniesiony aportem do spółki celowej. Takie rozwiązanie jednak ma wadę, gdyż może zwalniać całkowicie producentów z odpowiedzialności (a tym samym kłaść mniejszy nacisk na bezpieczeństwo produktu), co z resztą też zostało zauważone przez Habilitanta.

W tej części zdecydowanie zabrakło rozważań dotyczących rozwiązań proponowanych w innych systemach prawnych, ale przede wszystkim zabrakło omówienia działań podejmowanych na szczeblu Unii Europejskiej.

W dniu 20 października 2020 r. Parlament Europejski wydał Rezolucje z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję, w której podkreśla m.in., iż przyszłościowe ramy prawne odpowiedzialności cywilnej muszą wzbudzać zaufanie do bezpieczeństwa, niezawodności i spójności produktów i usług, w tym do technologii cyfrowej, aby zapewnić równowagę między skuteczną i sprawiedliwą ochroną potencjalnych poszkodowanych a jednoczesnym dawaniem wystarczającego pola do manewru, by umożliwić przedsiębiorstwom, w szczególności małym i średnim, rozwój nowych technologii, produktów i usług.

[8] Tak *P. Machnikowski,* Perspektywa uegulowania odpowiedzialności cywilnej związanej z nowymi technologiami, w: *A. Dańsko-Roesler, M. Leśniak, M. Skory, B. Sołtys,* Ius Est Ars Boni et Aequi, Księga pamiątkowa dedykowana Profesorowi Józefowi Frąckowiakowi, Wrocław 2018, s. 688.

28 dniu września 2022 r. Komisja Europejska przyjęła propozycję dyrektywy w sprawie odpowiedzialności za sztuczną inteligencję (*AI Liability Directive,* AILD). Uzupełnia i unowocześnia ona unijne ramy odpowiedzialności cywilnej, wprowadzając po raz pierwszy przepisy dotyczące szkód wyrządzonych przez systemy SI. Jej celem jest ustanowienie szerszej ochrony poszkodowanych systemów SI poprzez ułatwienie dochodzenia roszczeń o odszkodowanie, a także wspieranie sektora sztucznej inteligencji. Komisja zwraca uwagę, iż krajowe strategie dotyczące sztucznej inteligencji pokazują, że kilka państw członkowskich (Czechy, Włochy, Malta, Polska, Portugalia) rozważa, a nawet konkretnie planuje działania ustawodawcze dotyczące odpowiedzialności cywilnej za sztuczną inteligencję. Biorąc pod uwagę znaczne różnice między istniejącymi w poszczególnych państwach członkowskich przepisami dotyczącymi odpowiedzialności cywilnej, można oczekiwać, że krajowe prawodawstwa w zakresie odpowiedzialności cywilnej sztucznej inteligencji będą zgodne z istniejącymi różnymi podejściami krajowymi, co zwiększy fragmentację prawa. Stanowi to wyzwanie dla Unii Europejskiej, ponieważ wpłynie to na jednolity rynek. Firmy prowadzące handel transgraniczny zmuszone będą do ponoszenia kosztów związanych z ryzykiem stosowania systemów SI i konieczności dostosowania ich do różnych prawodawstw. W efekcie, niewiele z nich zdecyduje się na wykorzystywanie sztucznej inteligencji, co utrudni jej upowszechnienie na całym terytorium UE.

Pozostaje mieć nadzieje, iż Habilitant będzie kontynuował badania w tym zakresie. Istnieje bowiem wiele wątpliwości interpretacyjnych oraz potrzeba wypełnienia luki, zwłaszcza przy prowadzeniu badań interdyscyplinarnych.

Przykładem prowadzenia badań interdyscyplinarnych Habilitanta jest współpraca z prof. Gryzem z York University, z którym to badali kwestie dotyczące kryterium wyjaśnialności. W publikacji „*Black Box Algorithms and*

the Rights of Individuals: No Easy Solution to the 'Explainability' Problem" zaproponowano alternatywne podejście do rozwiązania problemu wyjaśnialności, opierające się na wprowadzeniu zasad ścisłej certyfikacji systemów AI. Na szczególne podkreślenie zasługują rozważania interdyscyplinarne w tym obszarze. Dokonując analizy aspektów technicznych Habilitant wskazuje jednocześnie na istniejące bariery prawne. Postuluje, by rozpocząć dyskusję na temat potrzeby kompleksowego uregulowania sposobu tworzenia, wdrażania i nadzorowania systemów ML. Czerpiąc z doświadczeń sektora IT, najbardziej zasadne wydaje się wprowadzenie modelu regulacyjnego, w którym wiodącą rolę będą odgrywać różnego rodzaju mechanizmy certyfikacji. Podstawą takiego modelu może być schemat certyfikacji systemów ML dopuszczający różne schematy certyfikacji systemów funkcjonujących na różnych rynkach. Wskazuje też, iż konieczne będzie wyodrębnienie określonej kategorii systemów, których decyzje mogą mieć wpływ na podstawowe prawa i wolności. Podkreślona została także rola tzw. *soft law*, w tym międzynarodowe normy i kodeksy postępowania, w celu wspierania rozwoju norm branżowych i mechanizmów samoregulacji.

Habilitant badał także problem tzw. robotyzacji, a zwałszcza jej wpływu na rynek pracy. Robotyzacja jest w ostatnich latach przedmiotem intensywnych badań w różnych obszarach nauki. W raporcie przygotowanym przez McKinsey Global Institute (MGI) wskazuje się na 12 obszarów techonologii, które mogą mieć ogromny wpływ na życie i pracę ludzi, a także na rozwój gospodarczy. Autorzy raportu starają się również oszacować potencjalny wpływ ekonomiczny każdej z tych technologii na zastosowania w 2025 r.[9] Wśród tych obszarów znalazły się, m.in. zaawansowana robotyka (automatyka) oraz autonomiczne lub

[9] Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy, Maj 2013 r. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Disruptive%20technologies/MGI_Disruptive_technologies_Full_report_May2013.ashx

częściowo autonomiczne pojazdy.

W 1942 r. Isaac Asimov jako pierwszy przedstawił trzy prawa robotyki. w swojej powieści Zabawa w berka (Runaround): „prawo pierwsze: robot nie może skrzywdzić człowieka, ani przez zaniechanie działania dopuścić, aby człowiek doznał krzywdy; prawo drugie: robot musi być posłuszny rozkazom człowieka, chyba że stoją one w sprzeczności z pierwszym prawem; prawo trzecie: robot musi chronić sam siebie, jeśli tylko nie stoi to w sprzeczności z pierwszym lub drugim prawem". W późniejszym czasie zostało dodane jeszcze „prawo zerowe", według którego robot nie może skrzywdzić ludzkości i nie może doprowadzić do uszczerbku dla ludzkości poprzez zaniechanie działania.

Prawa te stały się zarówno inspiracją, jak i podstawą dla trwającej obecnie debaty na szczeblu Unii Europejskiej na temat statusu prawnego robotów oraz odpowiedzialności cywilnej za szkody przez nie wyrządzone. W latach 2012 2014 prowadzone były badania w ramach projektu finansowanego w siódmym programie ramowym WE, pt. „Regulacja nowych technologii robotycznych robotyka wobec prawa i etyki. Wytyczne dotyczące regulacji robotyki"[10] Celem projektu było określenie praw i przepisów niezbędnych do wprowadzenia technologii robotycznych, w tym identyfikowanie implikacji prawnych i etycznych nowych technologii robotycznych i ustalanie, czy istniejące ramy prawne są adekwatne w kontekście konkretnego poziomu technologicznego. Raport opublikowany przez zespół ROBOLAW analizuje wpływ technologii robotycznych na prawa w Europie, w tym też kwestie związane z pojazdami automatycznymi, wskazując na konieczność wbudowania sztucznej inteligencji

[10] "Regulating emerging robotic technologies in Europe: Robotics facing law and ethics" (ROBOLAW). Strona projektu zob. : http://www.robolaw.eu

w same pojazdy a nie w system drogowy i pokazując istniejące obecnie bariery prawne.

W publikacji *Wpływ robotyzacji na rynek pracy i sektor ubezpieczeń społecznych* zostało wyraźnie zaznaczone, iż priorytetem powinno być obecnie ustalenie statusu prawnego inteligentnych robotów (biorąc pod uwagę istniejące obecnie różnice w poszczególnych krajach, np. nadanie robotowi obywatelstwa przez władze Arabii Saudyjskiej. Habilitant postuluje wprowadzenie nawet w ograniczonym zakresie podmiotowości osób elektronicznych. Działanie to nie powinno być interpretowane jako próba zrównania praw osób fizycznych i systemów elektronicznych, a bardziej jako próba sprawiedliwego podziału odpowiedzialności różnych podmiotów za działanie i funkcjonowanie inteligentnych robotów. Problematyka nadania podmiotowości prawnej robotom nie jest nowa. Wprawdzie Habilitant wskazuje na działania Parlamentu europejskiego w tym zakresie, ale rozważania te wydają się być nie w pełni pogłębione.

Komisja Europejska ma bowiem opracować w ciągu kilku najbliższych lat regulacje dotyczące odpowiedzialności cywilnej i statusu prawnego robotów, według zaleceń Parlamentu Europejskiego. W lutym 2017 r. w Parlamencie Europejskim odbyło się dwudniowe seminarium poświęcone rozwojowi robotyki oraz sztucznej inteligencji, w trakcie którego uczestnicy analizowali raport „Świat robotów w kontekście wyzwań prawa cywilnego" przygotowany przez komisję spraw prawnych JURI, a którego efektem było uchwalenie Rezolucji Parlamentu Europejskiego z dnia 16 lutego 2017 r.

zawierające zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki.[11]

Parlament wskazuje, że latach 2010–2014 średni wzrost sprzedaży robotów wynosił 17 % rocznie, a w 2014 r. sprzedaż wzrosła o 29 %, co stanowi najwyższy w historii wzrost sprzedaży z roku na rok, a ponadto w ciągu ostatnich dziesięciu lat trzykrotnie wzrosła liczba składanych wniosków patentowych dotyczących robotyki. W perspektywie długoterminowej, według Parlamentu, obecna tendencja do projektowania inteligentnych i autonomicznych maszyn, które można szkolić i które potrafią samodzielnie podejmować decyzje, niesie ze sobą nie tylko obietnicę korzyści gospodarczych, lecz także wiele obaw dotyczących ich bezpośredniego i pośredniego wpływu na całe społeczeństwo.

W Rezolucji czytamy, że obecne ramy prawne nie będą wystarczające do uwzględnienia szkód powodowanych przez roboty nowej generacji, czyli roboty wyposażone w zdolność dostosowywania się i uczenia się, z czym wiąże się pewien stopień nieprzewidywalności ich zachowania. Takie roboty będą w sposób niezależny uczyć się w oparciu o własne, zróżnicowane doświadczenia i wchodzić w interakcje z otoczeniem w jedyny w swoim rodzaju i nieprzewidywalny sposób.

Parlament proponuje, by odpowiedzialność za szkody spowodowane przez roboty była proporcjonalna do poziomu instrukcji, jakie wydano takiemu robotowi i stopnia jego autonomii. Parlament podkreśla istnieje potrzeby stworzenia powszechnie akceptowanych i elastycznych definicji pojęć „robot"

[11] 2015/2103(INL). Rezolucja zawiera zapisy dotyczące: zasad ogólnych dotyczących rozwoju robotyki i sztucznej inteligencji do celów cywilnych, badań i innowacji, zasad etycznych, utworzenia Agencji europejskiej, praw własności intelektualnej a przepływ danych, standaryzacji, bezpieczeństwa i ochrony, autonomicznych środków transportu, robotów do opieki, robotów medycznych, naprawiania i usprawniania organizmu ludzkiego, edukacji i zatrudnienia, wpływu na środowisko, odpowiedzialności.

i „sztuczna inteligencja", które nie będą utrudniać innowacji, podkreślając, że mamy do czynienia z szeroką kategorią pojęciową, która wymaga dodatkowych wyjaśnień. Przykładowo do rozwoju pojazdów autonomicznych należy podchodzić systemowo, gdyż wymagają one stworzenia infrastruktury i systemów sterowania, co z kolei wiąże się z koniecznością uzgodnienia wielu wymogów standaryzacyjnych.

Analizując podstawowe przesłanki odpowiedzialności, największy problem może stanowić związek przyczynowy, który trzeba będzie odnieść do działania maszyny, a nie działalności człowieka, co stanowi pole do rozważań nad kwestią maszyny jako podmiotu prawa. Problem bowiem dotyczy pociągnięcia do odpowiedzialności samej maszyny w przypadku, gdy robot będzie samodzielny, a jego działanie będzie sprzeczne z intencjami producenta. Parlament Europejski przedstawia propozycję rozwiązania tego problemu poprzez wprowadzenie osobowości elektronicznej, co umożliwi przypisanie odpowiedzialności maszynom. W Rezolucji Parlament posługuje się pojęciem osoby elektronicznej (dla najbardziej rozwiniętych robotów autonomicznych). Propozycja ta popierana jest przede wszystkim przez producentów, którzy unikną w ten sposób odpowiedzialności. Budzi jednak sprzeciw wielu podmiotów, zwłaszcza wśród ekspertów zajmujących się sztuczną inteligencją. Osobowość prawna wiąże się niejako automatycznie z przypisaniem praw i obowiązków, które są ściśle skorelowane z moralnością ludzką, a wobec tego jakie prawa może uzyskać robot? Parlament zauważa, że rozwój technologii w zakresie robotyki będzie wymagał większego zrozumienia potrzeby wspólnych podstaw koniecznych w związku z połączoną działalnością człowieka i robota, które powinny być oparte na dwóch stosunkach wzajemnej zależności, czyli przewidywalności i sterowalności, które mają znaczenie dla określenia, jakimi informacjami mają się dzielić ludzie i roboty oraz jak można uzyskać wspólne podstawy dla ludzi i robotów, aby umożliwić ich sprawne

połączone działanie. Parlament zwraca uwagę, że Komisja będzie musiała dokonać szczegółowej oceny w celu określenia, czy należy zastosować odpowiedzialność na zasadzie ryzyka, czy też podejście zakładające zarządzanie ryzykiem, które polega na skupieniu uwagi na osobie, która może, w określonych okolicznościach, zminimalizować ryzyko i podjąć działania w odniesieniu do negatywnych skutków. Proponuje się ponadto wprowadzenie systemu obowiązkowych ubezpieczeń dla producentów lub właścicieli robotów, który miałby zostać uzupełniony funduszem, z którego kompensowane byłyby szkody, nieobjęte ubezpieczeniem. Z utworzeniem takiego funduszu wiąże się kilka pytań: w jaki sposób miałby być zasilany? Jeśli ze składek, to kto miałby je płacić? Czy obejmowałby on wszystkie rodzaje robotów? Jak miałoby się to do odpowiedzialności producentów? Itp.

3. Wnioski końcowe

Habilitant nie napisał żadnej monografii (jedno lub wieloautorskiej), z wyjątkiem opublikowanej rozprawy doktorskiej. Nie był ani kierownikiem projektu ani członkiem żadnego zespołu badawczego w projekcie finansowanym ze źródeł zewnętrznych (np. NCN). Niemniej jednak odbył staż naukowy oraz wykazał dużą aktywność publikacyjną w dwóch ośrodkach naukowych.

W podsumowaniu należy stwierdzić, że oceniany dorobek naukowy jest zróżnicowany jakościowo, ale ogólnie **ocena wypada pozytywnie.**

IV. Ocena pozostałej aktywności naukowej, dorobku dydaktycznego i organizacyjnego oraz współpracy międzynarodowej

Aktywność Habilitanta związaną z uczestnictwem w konferencjach i seminariach krajowych i międzynarodowych należy ocenić jako niewystarczającą. Dr Rojszczak wziął czynny udział zaledwie w 17 konferencjach naukowych, w tym tylko jednej konferencji międzynarodowej.

Podobnie należy ocenić aktywność Habilitanta w zakresie współpracy międzynarodowej.

Cykl publikacji, wskazany jako osiągnięcie naukowe:

. – Sumaryczny IF 2021: 11,16

. – Sumaryczny SNIP 2021: 16,76

. – Sumaryczna punktacja MEiN: 1 500

Dorobek opublikowany po uzyskaniu stopnia doktora nauk prawnych:

. – Sumaryczny IF 2021: 16,574

. – Sumaryczny SNIP 2021: 28,113

. – Sumaryczna punktacja MEiN: ok. 2 900

Cytowania wg Google Scholar (2018-2023):

– cytowania: 140

– h-index: 7

– i10-index: 5

Liczba cytowań wydaje się być dość niska, zwłaszcza biorąc pod uwagę tematykę, która jest obecnie bardzo aktualna i pożądana przez naukowców w zakresie jej wykorzystania do swoich badań (nie tylko przez prawników). Po drugie, dziwi tak niska liczba cytowani, gdyż Habilitant opublikował swoje badania w czasopismach międzynarodowych będących w międzynarodowych bazach, w języku angielskim. Co do punktacji MEiN, z uwagi na zmieniające się zasady w ostatnich latach trudno jest dokonać jej obiektywnej oceny.

Habilitant podkreśla, iż pełni rolę promotora oraz recenzenta prac dyplomowych studentów kierunku Administracja (WAiNS PW), a także wskazuje, iż tematyka wypromowanych prac dotyczyła prawnej regulacji unijnego i krajowego systemu cyberbezpieczeństwa, prawa ochrony danych, regulacji nowych form przetwarzania danych (w tym Big Data/IoT). Nie została jednak wskazana ilość dotychczas wypromowanych magistrów czy licencjatów.

Brak także informacji co do pełnienia roli promotora pomocniczego w postępowaniu doktorskim.

Habilitant od 2018 r. uzyskał dwa wyróżnienia:

. Nagroda indywidualna II stopnia JM Rektora PW za osiągnięcia naukowe w latach 2019- 2020.

. Nagroda specjalna im. prof. Remigiusza Kaszubskiego za rok 2020

za działania na rzecz innowacyjnych rozwiązań w dziedzinie bankowości elektronicznej i prawa nowych technologii.

Ocena pracy dydaktycznej wypada pozytywnie. Dr Rojszczak wykłada w kilku instytucjach następujące przedmioty:

Uniwersytet Gdański (2023) - prowadzenie wykładów dla studentów Wydziału Prawa i Administracji (kierunek: kryminologia) - kursy:

„Cyberbezpieczeństwo" (studia dzienne oraz zaoczne),

„Cyberprzestępczość" (studia dzienne oraz zaoczne).

Naczelna Rada Adwokacka / izby adwokackie (2020 - nadal) prowadzenie szkoleń/wykładów dla adwokatów oraz aplikantów adwokackich z zakresu cyberbezpieczeństwa, gromadzenia dowodów elektronicznych oraz anonimowości w Internecie.

Politechnika Warszawska (od 2019 - nadal) prowadzenie zajęć dla studentów Wydziału Administracji i Nauk Społecznych oraz Wydziału Zarządzania (studia dzienne i zaoczne); wykłady/ćwiczenia z zakresu: prawa nowych technologii, ochrony danych osobowych, prawa łączności elektronicznej, cyberprzestępczości i cyberbezpieczeństwa. Przykładowe prowadzone kursy:

„Cyberbezpieczeństwo i cyberprzestępczość perspektywa prawna",

„Funkcjonowanie sieci łączności elektronicznej",

„Prawne aspekty łączności elektronicznej",

„Prawo do informacji a ochrona danych osobowych",

„Regulacje prawne w marketingu internetowym",

„Systemy i usługi informatyczne w administracji publicznej”,

„Wprowadzenie do prawa nowych technologii”.

Instytut Nauk Prawnych PAN (od 2019) prowadzenie wykładu dla słuchaczy kolejnych edycji studiów podyplomowych Prawo Nowych Technologii: *„Cyberprzestępczość i bezpieczeństwo w sieci Internet”.*

Uniwersytet Ekonomiczny w Poznaniu (od 2018) prowadzenie wykładu dla słuchaczy kolejnych edycji studiów podyplomowych z zakresu cyberprzestępczości oraz sektorowych przepisów prawnych w obszarze bezpieczeństwa informacji.

Dr Rojszczak jest również aktywny organizacyjnie, będąc członkiem komitetów organizacyjnych konferencji naukowych (pt. *„Ochrona tajemnicy adwokackiej w usługach online”* oraz 7th International Conference on the History and Philosophy of Computing) oraz członkiem Grupy roboczej ds. strategicznych kierunków zarządzania danymi, utworzonej przez Departament Zarządzania Danymi KPRM w ramach Zespołu zadaniowego do spraw realizacji „Programu otwierania danych na lata 2021-2027”. Ponadto, jest koordynatorem pracy Zespołu Prawa Nowych Technologii WAiNS. Celem działania zespołu jest promowanie i wspólne prowadzenie badań dotyczących prawa nowych technologii. Zespół prowadzi także działania popularyzatorskie, takie jak cykl „Spotkania z prawem nowych technologii”. Wreszcie, pełni też różne fukacje w ramach WAiNS PW: Pełnomocnik Dziekana ds. funduszy strukturalnych, Przewodniczący Komisji ds. weryfikacji danych w Bazie Wiedzy Politechniki Warszawskiej, Członek Komisji ds. Nauki oraz Członek Komisji ds. Programów Studiów. Brak jednak wskazania dokładnych dat pełnienia tych funkcji.

V. Konkluzja

Biorąc powyższe pod uwagę, należy stwierdzić, że zostały spełnione wszystkie kryteria określone w art. 219 p.s.w.n. dla nadania Panu dr. Marcinowi Rojszczakowi stopnia naukowego doktora habilitowanego nauk prawnych.