Prof. dr hab. Maciej Rogalski
Uczelnia Łazarskiego

Warszawa, 23 sierpnia 2023 r.

Recenzja

dorobku naukowego dra Marcina Rojszczaka, ze szczególnym uwzględnieniem osiągnięcia naukowego, będącego podstawą ubiegania się o nadanie stopnia naukowego doktora habilitowanego, w postaci cyklu powiązanych tematycznie artykułów naukowych pod tytułem *Standardy prawne stosowania nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej*, sporządzona w postępowaniu o nadanie stopnia doktora habilitowanego

1. Uwagi ogólne

Zgodnie z uchwałą nr 59/2023 r. Rady Dyscypliny Nauki Prawne Uniwersytetu Gdańskiego z dnia 26 czerwca 2023 r. w sprawie powołania komisji habilitacyjnej w postępowaniu w sprawie nadania dr Marcinowi Rojszczakowi stopnia doktora habilitowanego w dziedzinie nauk społecznych w dyscyplinie nauki prawne, powierzono mi funkcję recenzenta w tej komisji. Ocena zostanie dokonana w oparciu o kryteria sformułowane w art. 219 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, tj. Dz. U. z 2023 r. poz. 742 ze zm. Zgodnie z tym przepisem, stopień doktora habilitowanego nadaje się osobie, która posiada stopień doktora, posiada w dorobku osiągnięcia naukowe, stanowiące znaczny wkład w rozwój określonej dyscypliny oraz wykazuje się istotną aktywnością naukową realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury, w szczególności zagranicznej.

Ocena dorobku naukowego dra Marcina Rojszczaka dokonana zostanie na podstawie dokumentów dołączonych do wniosku o wszczęcie postępowania habilitacyjnego przygotowanych przez Habilitanta i przedłożonych mi z pismem Przewodniczącego Rady Dyscypliny Nauki Prawne prof. UG dr hab. Piotra Uziębło.

Zgodnie z dołączoną kopią odpisu dyplomu, Pan dr Marcina Rojszczaka uzyskał stopień naukowy doktora nauk prawnych w zakresie prawa, na podstawie rozprawy doktorskiej pt. *Ochrona prywatności w cyberprzestrzeni w prawie polskim i międzynarodowym z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji.* Promotorem pracy był dr hab. Cezary Banasiński a recenzentami dr hab. Czesław Martysz oraz prof. dr hab. Andrzej Wróbel. Stopień doktora został nadany uchwałą Instytutu Nauk Prawo-Administracyjnych Uniwersytetu Warszawskiego z dnia 8 października 2018 r.

2. Ocena cyklu powiązanych tematycznie artykułów naukowych przedstawionych jako osiągnięcie naukowe

Zgodnie z art. 219 ust. 1 pkt 2 lit. b ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, osiągnięcie naukowe może stanowić 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 ustawy Prawo o szkolnictwie wyższym i nauce. Dr Marcin Rojszczak przedstawił jako osiągnięcie naukowe w postępowaniu habilitacyjnym cykl artykułów pod ogólnym tytułem *Standardy prawne stosowania nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej.* Artykuły te były wydane w latach 2018-2023 w czasopismach naukowych, które znajdują się w wykazie przygotowanym zgodnie z przepisami wydanymi na podstawie art. 267 ust. 2 pkt 2 lit. b ustawy Prawo o szkolnictwie wyższym i nauce.

Na przedstawiony przez Habilitanta cykl powiązanych tematycznie artykułów naukowych składa się w sumie 19 artykułów, które zostały podzielone przez Habilitanta na pięć grup tematycznych:

1. Państwo demokratyczne a inwigilacja ukierunkowana:

1.1. *Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji*, Państwo i Prawo 2018, nr 10

1.2. *Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego,* Studia nad Autorytaryzmem i Totalitaryzmem 2020, nr 2

2. Europejski (unijny) standard zabezpieczeń systemowych:

2.1. *Extraterritorial Bulk Surveillance after the German BND Act Judgment*, European Constitutional Law Review 2021, nr 1

2.2. *The uncertain future of data retention laws in the EU: Is a legislative reset possible?*, Computer Law & Security Review 2021, nr 7

2.3. *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, European Constitutional Law Review 2021, nr 4

2.4. *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses,* European Journal of Crime, Criminal Law and Criminal Justice 2021, nr 4

2.5. *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* Studia Prawa Publicznego 2022, nr 4

3. Inwigilacja elektroniczna jako zagrożenie dla standardów państwa prawa – perspektywa krajowa:

3.1. *Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland,* Demokracy and Security 2020, nr 4

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

3.3. *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, nr 11

3.4. *Kontrola sądów krajowych nad stosowaniem środków inwigilacji elektronicznej na tle orzecznictwa ETPC,* Państwo i Prawo 2022, nr 4

3.5. *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna,* Państwo i Prawo 2023, nr 2

4. Doświadczenia innych państwa:

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

4.2. *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych,* Ius Novum 2019, nr 1

4.3. *The ECTHR's Judgment in Case of Centrum for Rättvisa v. Sveden as a Leading Case for the Review of Domestic Regulations on Signals Surveillance,* Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego 2019, vol. XVII

5. Inwigilacja elektroniczna w kontekście współpracy transgranicznej:

5.1. *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, nr 3

5.2. *Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace*, Information & Communication Technology Law 2021, nr 1

5.3. *CLOUD act agreements from an EU perspective,* Computer Law & Security Review 2020, nr 38

5.4. *e-Ewidence Cooperation in Criminal Matters from an EU Perspective,* Modern Law Review 2022, nr 4.

Habilitant nazwał cykl wymienionych artykułów *Standardy prawne stosowania nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej.* Zgodnie z tym zbiorczym tytułem przedmiotem analiz w tych artykułach są głównie zagadnienia dotyczące nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej w aspekcie ochrony podstawowych praw i wolności obywatelskich. Treść wybranych artykułów jest więc zgodna ze zbiorczym tytułem cyklu tych opracowań.

Habilitant w zakresie swoich badań stawia jako jedno z podstawowych pytań, w jaki sposób należy kontrolować stosowanie środków nieukierunkowanej inwigilacji aby ograniczyć ryzyko nadużycia władzy? Zakresem swoich badań obejmuje kwestie, czy koniecznym i niezbędnym środkiem dla ochrony państwa demokratycznego może być mechanizm, którego nie można pogodzić z fundamentalnymi wartościami ustrojowymi? Habilitant wyjaśnia, że w szerszym ujęciu celem jego badań była krytyczna analiza standardów stosowania środków inwigilacji elektronicznej stosowanych w państwach demokratycznych, zarówno w obszarze inwigilacji nieukierunkowanej, jak i inwigilacji ukierunkowanej, a także diagnoza zagrożeń związanych z upowszechnianiem różnych nadmiarowych form gromadzenia danych oraz ich wpływu na prawa podstawowe.

Habilitant wskazał, że wstępna hipoteza badawcza, koncentrowała się na ustaleniu, czy stosowanie środków inwigilacji nieukierunkowanej może być skutecznie kontrolowane w warunkach państwa demokratycznego. Wyjaśnił także, że kompleksowe omówienie tego zagadnienia wymaga odniesienia się również do środków inwigilacji ukierunkowanej, ponie-

waż, jak wyjaśnia Habilitant, w rzeczywistych zastosowaniach granica pomiędzy inwigilacją nieukierunkowaną a ukierunkowaną jest trudna do wyznaczenia. W ten sposób poszerzył zakres swoich badań pod względem przedmiotowym, poza wskazaną w tytule cyklu artykułów nieukierunkowaną inwigilacją elektroniczną, o inwigilację nieukierunkowaną.

Zakreślony w ten sposób obszar badawczy Habilitant analizował w cyklu powiązanych tematycznie artykułów, które podzielił na wskazane już wcześniej pięć grup obszarów badawczych.

W dalszej części recenzji zostanie przeprowadzona ocena poszczególnych artykułów według tematycznego podziału dokonanego przez Habilitanta.

Ad 1. Państwo demokratyczne a inwigilacja ukierunkowana.

1.1. *Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji*, Państwo i Prawo 2018, nr 10.

Na wstępie Autor wyjaśnia, że celem artykułu jest omówienie argumentów przedstawianych przez zwolenników programów inwigilacji elektronicznej, a w dalszej części artykułu doprecyzowuje że chodzi o masową inwigilację. Przedstawia kontrargumenty i krytykuje następujące tezy zwolenników inwigilacji: prywatność jest problemem pierwszego świata; masowa inwigilacja nie wyrządza szkody; tylko osoby zaangażowane w działania przestępcze muszą obawiać się inwigilacji; masowa inwigilacja jest potrzebna jako środek ochrony przed terroryzmem. We wnioskach końcowych negatywnie ocenia rozbudowę programów inwigilacyjnych. Podaje przykład Polski, która według Autora jest jednym z niewielu państw UE w którym nie wycofano z porządku prawnego ogólnego obowiązku retencji danych. Należy jednak zwrócić uwagę, że uregulowanie to badał TK, który wyrokiem z 30 lipca 2014 r., a więc już po wyroku z 8 kwietnia 2014 r. TSUE, który w połączonych sprawach C-293/12 i C-594/12, stwierdził nieważność dyrektywy 2006/24/WE, będącej podstawą wprowadzenia do polskiej ustawy Prawo telekomunikacyjne regulacje dotyczące retencji. Szkoda, że Autor nie wyjaśnił szerzej, czy i w jakim zakresie polski TK uwzględnił wskazany wyrok TSUE i dlaczego nie została stwierdzona ewentualna sprzeczność polskich przepisów Prawa telekomunikacyjnego w zakresie retencji z Konstytucją RP. Kwestia ta podnoszona jest także w literaturze.

1.2. *Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego,* Studia nad Autorytaryzmem i Totalitaryzmem 2020, nr 2.

W artykule tym Autor zajmuje się problemem dopuszczalnych granic inwigilacji w demokratycznym państwie. Koncentruje się na masowej inwigilacji elektronicznej. Formułuje

pytanie badawcze: czy niezależnie od wdrożonych zabezpieczeń prawnych sama koncepcja stosowania masowych środków inwigilacji elektronicznej może zostać pogodzona ze sposobem funkcjonowania państwa demokratycznego. Analizując granice dopuszczalnej inwigilacji w państwach demokratycznych przywołuje orzecznictwo ETPC i TSUE. W podsumowaniu, wskazuje negatywne zjawiska inwigilacji jak erozja „uzasadnionego oczekiwania prywatności" czy „przyzwyczajanie się do życia w środowisku nadzorowanych", gdzie brak transparentności w prowadzonych działaniach inwigilacyjnych traktowane są jako naturalny element funkcjonowania organów państwa. Autor powinien także jednoznacznie i szerzej odpowiedzieć na postawione pytanie badawcze, tj. czy jest możliwa, przy zastosowaniu odpowiednich zabezpieczeń prawnych i technologicznych, masowa inwigilacja elektroniczna w państwie demokratycznym.

2. Europejski (unijny) standard zabezpieczeń systemowych.

2.1. *Extraterritorial Bulk Surveillance after the German BND Act Judgment*, European Constitutional Law Review 2021, nr 1.

W artykule tym Autor zajmuje się kwestią uprawnień Federalnej Służby Wywiadowczej (BND), ale w zakresie wywiadu elektronicznego prowadzonego za granicą (foreign-foreign surveillance). Kwestia ta jest analizowana w artykule w związku z orzeczeniem niemieckiego Federalnego Trybunału Konstytucyjnego (FTK) z dnia 19 maja 2020 r. dotyczącego właśnie wywiadu elektronicznego prowadzonego za granicą. W szczególności Autor zajmuje się problemem odmiennych standardów inwigilacji w stosunku do własnych obywateli oraz obcokrajowców. W związku z tym najpierw w artykule w dwóch pierwszych częściach przedstawia różnice pomiędzy mechanizmami krajowej oraz zagranicznej kontroli oraz prezentuje podstawowe pojęcia z zakresu tej kontroli. Następnie przedstawia ewolucję orzecznictwa niemieckiego FTK w omawianym zakresie oraz orzeczenie z 19 maja 2020 r. Trudno nie zgodzić się z wnioskami Autora sformułowanymi w konkluzjach artykułu, że w demokratycznym państwie nie powinny być stosowane podwójne standardy, które są różne w zależności od tego jaka jest geograficzna lokalizacja osoby poddanej inwigilacji.

2.2. *The uncertain future of data retention laws in the EU: Is a legislative reset possible?*, Computer Law & Security Review 2021, nr 7.

W artykule tym Autor zajmuje się najnowszym europejskim orzecznictwem sądowym w sprawach w zakresie gromadzenia danych (data retention), zarówno na potrzeby bezpieczeństwa narodowego (orzeczenia: Privacy International, La Quadrature du Net), jak i zwalczania przestępczości kryminalnej (orzeczenie H.K.). Wyjaśnia że analiza orzecznictwa w

tym zakresie jest punktem wyjścia do dyskusji nad propozycją Rady UE, która może ograniczyć jurysdykcję sądową w sprawa dotyczących gromadzenia danych, jeżeli jest to związane z bezpieczeństwem narodowym. Z podsumowania wynika, że Autor podziela pogląd Court of Justice o potrzebie zapewnia balansu pomiędzy potrzebami zapewnienia bezpieczeństwa narodowego a przestrzeganiem standardów demokratycznego państwa, z naciskiem na tą drugą stronę balansu. Interesująca jest przybliżona przez Autora dyskusja, prowadzona w związku z orzeczeniem CJEU w sprawie La Quadrature du Net, gdzie francuska Council d'Etat zanegowała sposób retencyjny danych opisany w tym orzeczeniu, jako uniemożliwiający zapewnienia bezpieczeństwa narodowego Francji, które jest już zagrożone i naruszone przez ataki terrorystyczne w ostatnich latach. Odmienne stanowisko zajął belgijski Trybunał Konstytucyjny. Trafnie zauważa Autor, że z pewnością jest to problem, gdy najwyższe sądy narodowe w krajach UE dochodzą do całkowicie odmiennych wniosków w zakresie orzeczeń CJEU.

2.3. *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, European Constitutional Law Review 2021, nr 4.

W artykule tym Habilitant ponownie wraca do analizowanej już problematyki orzeczeń w sprawach Privacy International i La Quadrature du Net (LQN) oraz krytycznego stanowiska francuskiej Council d'Etat do tych orzeczeń. Część tego artykułu jest pewnym powtórzeniem wywodów zawartych w artykule *The uncertain future of data retention laws in the EU: Is a legislative reset possible?,* Computer Law & Security Review 2021, nr 7. Autor uważa, że przedstawiona wykładnia przepisów unijnych w sprawach Privacy International i LQN przez Trybunał Sprawiedliwości UE (CJEU) jest niewystarczająca aby zapewnić harmonizację w zakresie uchwalania i stosowania przepisów na poziomie krajowym, co może doprowadzić do dwóch standardów implementacji zasada gromadzenia danych (data retention). Wskazuje także odmienne podejście w orzecznictwie w zakresie prowadzenia inwigilacji oraz gromadzenia danych przez CJEU oraz Europejski Trybunał Praw Człowieka (ECHR). Ten pierwszy dopuszcza dalej idące środki w zakresie kontroli niż ten drugi. Autor proponuje znalezienie alternatywnych rozwiązań, swoistej „trzeciej drogi", która polegałby na nałożeniu na operatorów obowiązku „to pre-filter metada" na podstawie określonych reguł z kontrolą sądu. W praktyce rozwiązania to wydaje się być trudne do zrealizowania z uwagi na dużą ilość tego rodzaju operacji, a przede wszystkim dlatego, że operatorom jako podmiotom prywatnym byłyby przekazywane, przynajmniej w pewnym zakresie, kompetencje, które są zastrzeżone dla sądów.

2.4. *EU Criminal Law and Electronic Surveillance: The Pegasus System and Legal Challenges It Poses,* European Journal of Crime, Criminal Law and Criminal Justice 2021, nr 4.

Oprogramowanie Pegasus jest przyczynkiem do dokonania analizy obecnych regulacji w zakresie inwigilacji i udzielenie odpowiedzi na pytanie, czy korzystanie z tak nowoczesnych i stwarzających nowe możliwości techniczne rozwiązań jest pod właściwą kontrolą odpowiednich organów i zgodne z rządami prawa. W podsumowaniu Autor formułuje wnioski z którymi trudno się nie zgodzić a mianowicie, że z jednej strony, uprawnione służby powinno posiadać nowoczesne narzędzia technologiczne do walki z przestępczością a z drugiej strony wykorzystywanie tych narządzi musi być zgodne z podstawowymi standardami państwa prawa.

2.5. *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* Studia Prawa Publicznego 2022, nr 4.

Zgodnie z tytułem, Autor w tym artykule zajmuje się przeglądem i analizą orzecznictwa TSUE oraz ETPC w zakresie dopuszczalności stosowania nieukierunkowanych środków inwigilacji elektronicznej, w szczególności w aspekcie proporcjonalności przepisów krajowych w tym obszarze regulacji. Z pewnością wartościowe jest przybliżenie przez Autora problematyki, niezbyt często podejmowanej w polskie literaturze, a dotyczącej nieukierunkowanej inwigilacji stosowanej przez władze publiczne, rozumianej jako hurtowe monitorowanie łączności elektronicznej, wykorzystywanej w obszarze walki z przestępczością oraz ochroną bezpieczeństwa narodowego. Celem tego artykułu jest jak wyjaśnia Autor, przybliżenie ewolucji standardu inwigilacji elektronicznej w najnowszym orzecznictwie. Artykuł ten stanowi kontynuację artykułu opublikowanego w 2017 r. w Studiach Prawa Publicznego. Autor krytycznie ocenia orzeczenie ETPC w sprawie *Big Brother Watch,* w którym Trybunał w celu ochrony bezpieczeństwa narodowego dopuszcza możliwość przechwytywania hurtowego danych. Przywołuje także orzeczenie ETPC w sprawie *Centrum för rättvisa.* Według Autora występuje brak spójności pomiędzy kierunkiem orzecznictwa ETPC a standardem stosowanym przez TSUE, uznając, że TSUE ustanawia wyższy poziom ochrony.

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

3.1. *Surveillance, Legal Restraints and Dismantling Democracy: Lessons from Poland,* Demokracy and Security 2020, nr 4.

Przedmiotem artykułu jest analiza na przykładzie Polski, gdzie według Autora model wykorzystania środków w zakresie inwigilacji oparty na zasadzie „checks and balances" nie

funkcjonuje, ponieważ rząd Polski narusza rządy prawa, zmierzając w kierunku rządów autorytarnych. Autor wyjaśnia, że celem tego artykułu jest wskazanie na przykładzie Polski, gdzie dokonywane są zmiany w przepisach prawa, znaczenia istnienia realnych zabezpieczeń prawnych, których celem jest ograniczenie zakresu inwigilacji w demokratycznych państwach. W konkluzjach artykułu Autor opowiada się za zwiększeniem kompetencji unijnych instytucji, aby w sposób szybki i skuteczny reagować na naruszenia prawa w państwie członkowskim UE.

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

Artykuł dotyczy zmian w polskich przepisach podatkowych zezwalających na wykorzystywanie nowych programów IT, a konkretnie programu STIR (System Teleinformatyczny Izby Rozliczeniowej), w walce z poważną przestępczością finansową (wykrywanie przestępstw finansowych i podatkowych). Celem artykułu jest ocena STIR z punktu widzenia podstawowych praw człowieka, w szczególności w zakresie prawa do prywatności. Autor zwraca uwagę, że artykuł może stanowić kontynuację rozważań w innym artykule autorstwa M. Papis-Almansa. W podsumowaniu Autor formułuje wnioski, które trudno nie zaakceptować. Wskazuje z jednej strony na konieczność posiadania przez państwa odpowiednich narzędzi pozwalających na skuteczną walkę z przestępczością finansową, w szczególności z VAT-owską, a z drugiej strony na potrzebę wykorzystania STIR zgodnie z podstawowymi standardami ochrony praw człowieka, interpretowanymi zgodnie z orzecznictwem sądów UE.

3.3. *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, nr 11.

W artykule tym Autor ponownie wraca do wyroku C-746/18, H.K. Zajmuje się przede wszystkim kwestią, według Autora, skutków tolerowania od lat niegodności przepisów retencyjnych w związku z dotychczasowym orzecznictwem sądów UE, przez krajowego prawodawcę. Zwraca uwagę, że „z uwagi na trwający w Polsce kryzys ustrojowy rozstrzygniecie narastających wątpliwości dotyczących sposobu wykonywania uprawnień inwigilacyjnych państwa poprzez kontrolę przeprowadzoną przez sąd konstytucyjny jest znacząco utrudnione". W recenzji zwrócono już uwagę, że kwestią tą miał okazję już zająć się TK, jeszcze w wyroku z 30 lipca 2014 r.

Celem tego artykułu dla Autora jest odniesienie do modelu prawnego funkcjonującego w Polsce, w aspekcie standardu orzeczniczego TS, w zakresie zgodności stosowania inwigila-

cji elektronicznej z prawem UE. Autor krytykuje polskie uregulowania, z uwagi na brak konsekwencji, w zakresie dostępu uprawnionych organów do tzw. metadanych pochodzących z łączności elektronicznej, a więc danych o ruchu oraz lokalizacji niestanowiących merytorycznej treści przekazu. Autor zwraca uwagę, że dostęp ten nie jest poprzedzony żadną formą kontroli sądowej. Natomiast w przypadku dostępu do treści przekazywanych informacji, standardem jest wymóg uzyskania zgody właściwego sądu (kontrola ex ante).

3.4. *Kontrola sądów krajowych nad stosowaniem środków inwigilacji elektronicznej na tle orzecznictwa ETPC,* Państwo i Prawo 2022, nr 4.

Autor w artykule zajmuje się, zgodnie z tytułem, kontrolą sądową w Polsce nad stosowaniem środków inwigilacji elektronicznej. Zajmuje się tą tematyką w szczególności z uwagi na przyjęcie w 2016 r. dwóch ustaw: ustawy o zmianie ustawy o Policji oraz innych ustaw oraz ustawy o działaniach terrorystycznych. Nowela ustawy o policji wynikała z wyroku TK z 30 lipca 2014 r. Autor uważa, że sposób prowadzenia kontroli sądowej daleki jest od standardów wskazanych z orzecznictwie ETPC. Przyznaje jednak trafnie, że nie tylko jest to kwestia uregulowań prawnych, ale też praktyki sądowej, gdzie sądy ograniczają się swoją funkcję kontrolną do akceptowania wniosków i sprawozdań przedstawianych przez uprawnione do kontroli organy. We wnioskach końcowych słusznie zauważa, że sądy obecnie już posiadają odpowiednie narzędzia kontroli. Autor jako cel artykułu wskazuje porównanie praktyki krajowej ze standardami ETPC. Zauważyć należy, że Autor ponownie analizuje te same orzeczenia, które już w innych artykułach analizował (*Big Brother Watch, Centrum för rättvisa*, zob. *Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka,* Studia Prawa Publicznego 2022, nr 4).

3.5. *Wadliwe dowody z retencji danych telekomunikacyjnych a polska procedura karna,* Państwo i Prawo 2023, nr 2.

Autor ponownie na kanwie orzecznictwa TSUE zajmuje się kwestią retencji danych telekomunikacyjnych. Opisuje sprawę *Dwyer* z kwietnia 2022 r., ale także już wcześniej opisywane sprawy *LQN* czy *Tele2 Sverige, Digital Rights Ireland.* Autor formułuje następujący problem, którym się zajmuje w artykule: jakie skutki mogą zaistnieć, w następstwie zaniedbań ustawodawcy w zakresie nowelizacji przepisów dotyczących retencji danych w Polsce, w zakresie nie tylko trwających postępowań karnych, ale już zakończonych. W podsumowaniu Autor wskazuje, że minęło już wiele lat od wydania wyroku z 2006 r. przez TSUE w sprawie wadliwych przepisów retencyjnych zawartych w dyrektywie UE, a polski rząd miał dużo czasu aby zmienić przepisy prawa. Autor zauważa także, że nie przeprowadzono także

kontroli przez TK. Ponownie należy przywołać wyrok TK z 30 lipca 2014 r. Z uwagi na sformułowany problem badawczy wpływu uregulowań w zakresie retencji danych na trwające i zakończone postępowania karnego, Autor powinien się zająć tą kwestią w sposób bardziej pogłębiony (szerzej pisze w zasadzie tylko o art. 540 k.p.k.). Warto byłoby się odniesień szerzej niż to uczynił Autor do uregulowań k.p.k. w zakresie dowodów, ich oceny przez sąd, obowiązujących zasad procesowych, praktycznych problemów zaistniałej sytuacji na ocenę odpowiedzialności oskarżonego itp.

4. Doświadczenia innych państwa.

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

4.2. *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych,* Ius Novum 2019, nr 1.

4.3. *The ECTHR's Judgment in Case of Centrum for Rattvisa v. Sveden as a Leading Case for the Review of Domestic Regulations on Signals Surveillance,* Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego 2019, vol. XVII.

W cyklu tych trzech artykułów Autor przybliża uregulowania w zakresie inwigilacji w UK, USA oraz Szwecji, głównie znowu, z perspektywy orzecznictwa sądów unijnych. W pierwszym z tych artykułów Autor prowadzi rozważania, jakie konsekwencje dla stosowania inwigilacji w UK, będzie miał Brexit z uwagi na to, że poprzez opuszczenie UE przez UK, przestały obowiązywać uregulowania unijne i dorobek orzeczniczy sądów unijnych. Zagrożenia jakie w związku z tym dostrzega Autor polegać mają na większym rozwoju uprawnień w zakresie prowadzenia inwigilacji organów państwowych, przy jednoczesnym ograniczonym wpływie orzecznictwa TSUE oraz długo trwających postępowaniach przed ETPC.

W drugim artykule dokonuje ciekawej analizy prawnoporównawczej przepisów obowiązujących w UE z przepisami obowiązującymi w USA w zakresie ochrony danych osobowych, czy szerzej ochrony prywatności. W USA jest prezentowane odmienne podejście, tj. dopuszczające znacznie szerszy zakresie możliwość prowadzenia przez organy władzy publicznej programów inwigilacyjnych w oparciu o hurtowe i nieukierunkowane przechwytywanie danych. W podsumowaniu Autor wskazuje na kluczowe różnice pomiędzy prawodawstwem USA a regulacjami wynikającymi z EKPC oraz obowiązującymi na terenie UE, w odniesieniu do możliwości, zakresu i podstaw prawnych prowadzenia masowych programów inwigilacyjnych, np. na brak na poziomie konstytucji ochrony prawa do prywatności w USA

czy specjalny sąd w USA działający według określonej procedury zajmujący się sprawami inwigilacji, które to różnice są krytycznie oceniane przez Autora na niekorzyść USA. Autor wskazuje, że prawodawstwo USA nie wypełnia większości warunków minimalnych określonych w orzecznictwie ETPC czy TSUE w zakresie stosowania środków masowej inwigilacji przez organy władzy publicznej. W związku z tym można postawić pytanie, czy państwo, które stosuje takie odmienne pod względem prawnym rozwiązania jak UE i odmienne od praktyki orzeczniczej ETPC czy TSUE, należy uznać za niedemokratyczne (czy USA są państwem autorytarnym)?

W trzecim artykule Autor ponownie omawia, przedstawiane już w innych własnych artykułach, orzeczenie ETPC w sprawie *Centrum för Rättvisa*. W orzeczeniu tym ETPC zaakceptował szwedzki model prowadzenia czynności inwigilacyjnych. Zaakceptowany szwedzki model inwigilacje stanowi ewolucję w kierunku, który uwzględnia argumenty zwolenników wzmocnienia uprawnień państwa w zakresie zapewnienia bezpieczeństwa narodowego.

5. Inwigilacja elektroniczna w kontekście współpracy transgranicznej.

5.1. *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, nr 3.

W artykule tym Autor podejmuje już wcześniej omawiany w swoich artykułach problem konfliktu pomiędzy bezpieczeństwem narodowym a prawem do prywatności w USA i UE. Celem artykułu, według Autora, jest określenie przyczyn problemów we współpracy UE-USA w zakresie ochrony prywatności i określenie możliwych rozwiązań. W konkluzjach Autor uważa, że USA nie ograniczą kompetencji i uprawnień organów władzy publicznej w obszarze bezpieczeństwa narodowego, uznając tę sytuację za niekorzystną, a jednym z dwóch powodów takie stanu rzeczy jest, według Autora, rządząca wtedy, tj. w chwili pisania artykułu administracja amerykańska. Trafnie wskazuje, na końcu podsumowania, cytując wypowiedzi innych, że musi zachodzić równowaga pomiędzy prawami jednostki a bezpieczeństwem narodowym", ale czy spojrzenie głownie z perspektywy unijnej i krytyczna ocena prawodawstwa i rozwiązań w USA nie jest stanowi naruszenie takiego balansu?

5.2. *Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace*, Information & Communication Technology Law 2021, nr 1.

Przedmiotem artykułu jest kwestia, czy i w jakim zakresie istniejące mechanizmy ochrony prywatności, w szczególności w UE, chronią prywatność w międzynarodowej cyberprzestrzeni (w relacjach międzynarodowych). Autor słusznie zauważa, że z uwagi na pozycję ekono-

miczną w świecie UE trudno jest i będzie narzucić pozostałym krajom świata standard ochrony prywatności funkcjonujący w UE. Pytanie, które można postawić, to czy standard UE w zakresie ochrony danych jest tym, który powinien obowiązywać pozostałe kraje? Słusznie zwraca uwagę Autor, że obecnie prywatność i jej naruszenie jest różnie rozumiane w UE, USA czy Chinach. Proponuje m.in. powołanie nowego międzynarodowego podmiotu, który zajmowałby się kwestiami ochrony prywatności i danych osobowych.

5.3. *CLOUD act agreements from an EU perspective,* Computer Law & Security Review 2020, nr 38.

Celem artykułu jest analiza CLOUD Act i CLOUD Act umów z perspektywy prawa EU, dla pokazania różnić w zakresie modeli ochrony danych i prywatności funkcjonujących w UE i USA. W artykule tym Autor szczegółowo analizuje CLOUD Act.

5.4. *e-Ewidence Cooperation in Criminal Matters from an EU Perspective,* Modern Law Review 2022, nr 4.

W artykule tym Autor omawia trzy opracowywane mechanizmy współpracy międzynarodowej: unijne rozporządzenie o dowodach elektronicznych; Drugi Protokół Dodatkowy do Konwencji Rady Europy o Cyberprzestępczości; projekt umowy UE-USA według modelu wynikającego z federalnej ustawy CLOUD Act. Wszystkie te akty wprowadzają nowe formy współpracy, których podstawowym elementem wyróżniającym jest to, że nakaz przekazywania danych jest kierowany bezpośrednio do zagranicznego dostawcy usługi. Autor zwraca uwagę na ryzyka związane z kontrolą celu wykorzystania przekazanych w ten sposób danych.

Niedawno, gdyż 12 lipca 2023 r., zostało przyjęte rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. UE L 191/118). Z uwagi na czas publikacji rozporządzenia, Habilitant nie mógł go uwzględnić. Mógł jednak podjąć szerszą analizę projektu z dnia 17 kwietnia 2018 r. (COM(2018) 225 final, 2018/0108 (COD) rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych. Analiza tego rozporządzenia w fazie projektu mogłaby być pomocna w aspekcie analizy prowadzonej w artykule *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, nr 11, gdzie Autor krytykuje zróżnicowanie wyrażania zgodny przez różne organy w zależności od rodzaju danych. Czy w związku z tym Komisja Europejska przygotowując projekt przewidujący takie zróżnicowanie (sąd lub prokurator wyrażający zgodę w zależności od rodzaju danych) działała niezgodnie z orzecznictwem TSUE i ETPC?

Prowadzone przez Habilitanta badania doprowadziły Go do następujących wniosków:

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; w efekcie wiele nowoczesnych technologii, wykorzystywanych w różnych obszarach, posiada potencjał inwigilacyjny.
4. Rosnącym zdolnościom inwigilacyjnym państw musi odpowiadać ustanowienie spójnego i ponadnarodowego modelu zabezpieczeń prawnych, podlegającego skutecznym mechanizmom 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 wprowadzonych w ostatnich latach zbliża Polskę do rozwiązań znanych z państw wprost autorytarnych.

W ramach cyklu artykułów podejmuje Habilitant różne zagadnienia badawcze, które dotyczące przewodniego zagadnienia, czyli wpływu stosowania środków nieukierunkowanej inwigilacji na podstawowe prawa i wolności obywatelskich oraz możliwość nadużycia władzy. Z punktu widzenia metodologii prowadzonej analizy, pewne wątpliwości może budzić podejście Autora, które wyraża się w poszukiwaniu w przypadku praktycznie każdej regulacji w zakresie nieukierunkowanej inwigilacji elektronicznej naruszenia praw obywatelskich lub nadużycia władzy. Z jednej stron trudno odmówić tego rodzaju podejściu uzasadnienia naukowego, tj. weryfikacji tych rozwiązań z punktu widzenia uregulowań prawnych, ale czasami

odbywa się kosztem pogłębionej analizy także przyczyn wprowadzenia danych regulacji, ich uzasadnienia i jakich wartości ochronie mają służyć, a także możliwych rozwiązań pozwalających na zabezpieczenie się przed ewentualnymi nadużyciami. W sposób nieunikniony pojawia się tu konflikt wartości w postaci ochrony prywatności obywateli, ale z drugiej strony zapewnienia bezpieczeństwa państwa i ich obywateli. Odpowiednie organy i służby muszą mieć narzędzia, które pozwolą skutecznie walczyć z tymi zagrożeniami, zwłaszcza w czasach terroryzmu i wojny w Ukrainie. Przykładem jest podejście prezentowane w USA, ale także pojawiające się stanowiska (orzeczenia) we Francji, a nawet w Szwecji. Autor nie zawsze poświęca wystarczająco dużo miejsca na analizę tych kwestii, w przeciwieństwie do ochrony praw obywatelskich.

Problem inwigilacji elektronicznej w aspekcie podstawowych praw obywatelskich był i jest często podejmowany w literaturze. Problematyce tej poświęcone są także monografie. W artykułach Habilitanta jest analizowane jednak dość nowe, związane z rozwojem technologicznym zagadnienie, dotyczące tzw. niekierunkowej inwigilacji elektronicznej. Zagadnienie to było w literaturze omawiane raczej przy okazji prezentowania zagadnień związanych z inwigilacją elektroniczną, a nie jako odrębne zagadnienia. Z pewnością więc te opracowania wypełniają lukę w tym obszarze w polskiej literaturze. Z drugiej strony pewna część artykułów stanowi omówienie orzecznictwa TSUE i ETPC. Niektóre rozważania w artykułach się powtarzają. Czasami można odnieść wrażenie, że artykuły w niektórych fragmentach, zwłaszcza dotyczących Polski, mają charakter rozważań bardziej politologicznych niż prawnych.

W sumie objętość artykułów to 437 stron. Wszystkie artykuły zawarte w cyklu publikacji podlegały standardowej podwójnej recenzji. Spośród 19 artykułów 9 ukazało się w międzynarodowych, wysoko punktowanych czasopismach naukowych. We wszystkich artykułach jest wykorzystana liczna literatura, w szczególności zagraniczna.

Wskaźnik cytowań artykułów zawartych w cyklu powiązanych tematycznie artykułów na temat nieukierunkowanej inwigilacji w latach 2018-2023 wyniósł: indeks Hirscha = 7 a i10-index =5. Natomiast sumaryczna punktacja MEiN 1 500.

Pomimo pewnych krytycznych uwag, cykl powiązanych tematycznie artykułów naukowych przedłożonych przez dra Marcina Rojszczaka jako osiągnięcie naukowe spełnia warunki stawiane tego rodzaju publikacjom. Cykl artykułów kwalifikuje się do oceny jako wnoszący znaczący wkład w rozwój dyscypliny nauki prawne.

3. Ocena pozostałego dorobku naukowego i aktywności Habilitanta

Dr Marcin Rojszczak uzyskał tytuł doktora nauk prawnych w zakresie prawa w 2018 r. Do wszczęcia postępowania habilitacyjnego w 2023 r. upłynęło więc 5 lat. Dorobek naukowy zgromadzony w tym okresie obejmuje 42 prace naukowe. Z tych 42 publikacji 19 składają się na przedstawiony cykl publikacji. Pozostałe więc publikacje stanowią 23 pozycje. Spośród tych 23 opracowań: 10 to artykuły, w tym 4 we współautorstwie; 9 rozdziały w pracach zbiorowych; 3 współredakcja opracowań zbiorowych; 1 monografia. Wszystkie 10 artykułów było opublikowanych w recenzowanych, prestiżowych czasopismach naukowych, w tym 6 w zagranicznych.

W zakresie pozostałego dorobku habilitacyjnego Autor koncentruje się na pięciu obszarach badawczych. Pierwszy obszar badawczy, dotyczy unijnego modelu cyberbezpieczeństwa i łączności elektronicznej. Zagadnieniom tym jest poświęcone najwięcej publikacji – 11. W publikacjach z tego obszaru Autor zajmuje się szeregiem zagadnień związanych z cyberbezpieczeństwem. Podejmuje problematykę cyberbezpieczeństwa z perspektywy przedsiębiorców, użytkowników i ochrony zdrowia. Zajmuje się modelem cyberbezpieczeństwa w UE oraz regulacjami unijnymi w tym zakresie. Szczegółowymi kwestiami dotyczącymi unijnych regulacji określonych produktów i usług, jak usługi OTT czy IoT. Praktyką w zakresie ataków i obrony w cyberbezpieczństwa. Słusznie zwraca uwagę, że istotnym elementem modelu cyberbezpieczeństwa jest ochrona infrastruktury krytycznej, gdyż niezbędne jest zapewnienia ciągłości świadczenia podstawowych usług dla ludności. Istotnym także elementem jest zapewnienie ochrony informacji stanowiących tajemnicę przedsiębiorstwa oraz danych klientów przedsiębiorstw. Zajmuje się także ważnym zagadnieniem, w związku z wejściem w życie dyrektywy Europejski Kodeks Łączności Elektronicznej (EECC), nowej, poszerzonej definicji usługi łączności elektronicznej oraz wpływu nowego kodeksu na dotychczasowe regulacje w obszarze łączności elektronicznej. Słusznie zauważa, że coraz większym zagrożeniem dla prywatności są nie tylko cyberataki na dostawców usług internetowych, ale podatności istniejące w produktach konsumenckich.

Drugi obszar badawczy Habilitanta związany jest głównie z praktycznymi zagadnieniami dotyczącymi cyberbezpieczeństwa w kancelariach prawnych, w tym w ujęciu cyberbezpieczeństwa jako czynnika zarządzania ryzykiem w kancelarii. Zagadnieniom tym poświęcone są tylko dwie publikacje. W pierwszej pracy (*Praktyczne aspekty* cyberbezpieczeństwa) Autor promuje zasady tzw. cyberhigieny. Opracowanie to stanowi rodzaj praktycznego

przewodnika postępowania dla prawników (adwokatów), który wyjaśnia różne obszary wykorzystywania w pracy prawnika nowych technologii. Z pewnością posiada to opracowanie dużą przydatność praktyczną.

Trzeci obszar badawczy dotyczy problematyki prywatności i prawa do ochrony danych. Kwestiom tym poświęcone są cztery publikacje, w tym monografia pt. *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji,* Warszawa 2019, s. 540. W zakresie całego pozostałego dorobku posiada ona największe znaczenie. W monografii Autor przedstawia najważniejsze regulacje dotyczące ochrony prywatności i danych osobowych w zakresie takich form przetwarzania danych, jak *cloud computing* czy *big data*. Autor przedstawia istniejące i projektowane regulacje, zarówno krajowe, jak i unijne. Zajmuje się także problematyką prywatności w aspekcie bezpieczeństwa publicznego. Ciekawą część pracy stanowią rozważania dotyczące programów masowej inwigilacji. W pozostałych publikacjach z tego obszaru zainteresowań Autor podejmuje problematykę ochrony prywatności i danych osobowych w aspekcie konkretnych rozwiązań technologicznych, jak Big Data czy blockchain. Podnosi problem regulacji rynku big data, w aspekcie zagrożeń związanych z inwigilacją, z uwagi na duże bazy danych o osobach, które ta technologia ze swojej istoty umożliwia gromadzić. Zwraca także uwagę na ważny aspekt związany z inwigilacją. W UE uwaga koncentruje się przede wszystkim na działalności organów publicznych prowadzących inwigilację, podczas gdy inwigilacja może być prowadzona także przez korporacje technologiczne. Do kwestii tych szczególną wagę przywiązuje się w USA.

Czwarty obszar badawczy został nazwany przez Autora jako prawna regulacja technologii przełomowych (*emerging technologies*). Zagadnieniom tym poświęcone są cztery publikacje. W opracowaniach tych Autor podejmuje m.in. problem wpływu robotyzacji na rynek pracy i sektor ubezpieczeń społecznych oraz zagadnienia związane ze sztuczną inteligencją w aspekcie prawnym i finansowym. W aspekcie prawnym badań nad sztuczną inteligencją Autor zajmuje się problematyką wyjaśnialności decyzji podejmowanych algorytmicznie. Problemem wyjaśnialności zajmuje się także w artykule *Black Box Algorithms and the Rights of Individuals: No Easy Solution to the Explainability Problem.* W aspekcie finansowym wykorzystania sztucznej inteligencji Autor zajmuje się ekonomicznymi skutkami rozpowszechniania systemów AI.

Wreszcie piąty obszar dotyczy problematyki nowych technologii w aspekcie ochrony praw podstawowych. Zagadnieniom tym poświęcone dwa artykuły. W pierwszym omawia

rolę urzędu ochrony konkurencji w ochronie wolności słowa. W drugim zagadnienie wspierania rodziny jako cel krajowej ustawy o leczeniu niepłodności w aspekcie indywidualnych praw podstawowych.

Oceniając pozostały dorobek można posłużyć się dwoma kryteriami: ilościowym i jakościowym. Oceniając go pod względem ilościowym, raczej trudno zakwalifikować go jako przesadnie obszerny. Należy jednak uwzględnić okres czasu w którym powstał, tj. relatywnie krótki, co z pewnością powinno wpływać korzystniej na taką ocenę. Kryterium ilościowe nie powinno być jednak decydującym. Należy przede wszystkim skoncentrować się na ocenie jakościowej tych rezultatów aktywności naukowo-badawczej Habilitanta. Publikacje Habilitanta należy uznać za interesujące i poruszające ważne zagadnienia. W znacznej części tych publikacji, poza prezentowanymi zagadnieniami teoretycznym są przedstawiane kwestie praktyczne. Autor wyjaśnił, że wykształcenie techniczne i dotychczasowe doświadczenia zawodowe powodują, że w tych opracowaniach koncentruje się na różnych aspektach prawnych regulacji w zakresie nowoczesnych technologii, a w szczególności zagadnieniach cyberbezpieczeństwa. Stwierdzić należy, że opublikowane przez Habilitanta po uzyskaniu stopnia doktora prace prezentują odpowiedni poziom naukowy i dobrze rokują na przyszłość w zakresie Jego dalszego rozwoju naukowego.

Po uzyskaniu stopnia doktora, Habilitant wystąpił z referatami na 16 krajowych konferencjach naukowych i na 1 konferencji zagranicznej. Wygłoszone przez Habilitanta referaty dotyczyły głównie problematyki poruszanej także w publikacjach, jak cyberbezpieczeństwo, inwigilacja czy sztuczna inteligencja.

Habilitant nie kierował międzynarodowymi i krajowymi projektami badawczymi. Nie wykazał także udziału w takich projektach.

4. Osiągnięcia w zakresie dorobku dydaktycznego, organizacyjnego, popularyzatorskiego i współpracy międzynarodowej

Dr Marcin Rojszczak odbył staż naukowy w Katedrze Prawa Informatycznego WPiA Uniwersytetu Gdańskiego („UG"). Współpracował także naukowo z UG w zakresie przygotowania monografii (*Nowe technologie w praktyce prawnika*) i konferencji (*Rok z RODO*). Nie odbywał stażów zagranicznych. Nie wskazał także współpracy naukowej z innymi ośrodkami naukowymi poza UG (współpracował tylko z prof. Gryzem nad przygotowaniem wspólnego artykułu). Współpracuje z Naczelną Radą Adwokacką w zakresie cyberbezpie-

czeństwa świadczenia usług prawnych. Efektem tej współpracy było opracowanie: *Dobre praktyki dotyczące cyberbezpieczeństwa w działalności kancelarii adwokackich i pracy adwokata.*

Doświadczenie dydaktyczne dr Marcina Rojszczaka nie jest duże. Od 2018 r. prowadzi wykład na studiach podyplomowych z zakresu cyberbezpieczeństwa na Uniwersytecie Ekonomicznym w Poznaniu. Od 2019 r. prowadzi w szerszym zakresie, na Politechnice Warszawskiej („PW") na Wydziale Administracji i Nauk Społecznych („WAiNS") oraz na Wydziale Zarządzania, zajęcia z prawa nowych technologii, ochrony danych osobowych, prawa łączności elektronicznej, cyberprzestępczości i cyberbezpieczeństwa. Od tego roku prowadzi także wykład na studiach podyplomowych w Instytucie Nauk Prawnych PAN. Prowadzi także od 2020 r. szkolenia dla adwokatów z zakresu cyberbezpieczeństwa. Od 2023 prowadzi wykłady na Uniwersytecie Gdańskim z zakresu cyberbezpieczeństwa i cyberprzestępczości. Pełnił także rolę promotora prac dyplomowych studentów kierunku administracja (WAiNS PW), z zakresu prawnych regulacji unijnego i krajowego systemu cyberbezpieczeństwa.

Dr Marcin Rojszczak na WAiNS PW pełnił funkcje pełnomocnika Dziekana ds. funduszy strukturalnych, przewodniczącego Komisji ds. weryfikacji danych w Bazie Wiedzy Politechniki Warszawskie, Członka Komisji ds. Nauki i Członka Komisji ds. Programów Studiów. Był współorganizatorem jednej ogólnopolskiej konferencji naukowej oraz członkiem komitetu organizacyjnego jednej międzynarodowej konferencji naukowej. Jest także członkiem Grupy roboczej ds. strategicznych kierunków zarządzania danymi utworzonej przez Departament Zarządzania Danymi KPRM oraz koordynuje prace Zespołu Prawa Nowych Technologii WAiNS.

W zakresie osiągnięć popularyzujących naukę wskazać należy na cykl „Spotkania z prawem nowych technologii" dla studentów PW, którego jest współorganizatorem. Udział w panelach organizowanych przez koła studenckie. Wywiady i komentarze prasowe, które Habilitant wskazał jako przykładowe cztery.

Habilitant jest również współredaktorem czasopisma Internetowy Kwartalnik Antymonopolowy i Regulacyjny, recenzentem artykułów w czasopismach krajowych i zagranicznych.

Dr Marcin Rojszczak otrzymał nagrodę Rektora PW za osiągniecia naukowe oraz nagrodę prof. R, Kaszubskiego za działalność na rzecz innowacyjnych rozwiązań w dziedzinie prawa nowych technologii.

5. Konkluzje

Zgodnie z postanowieniami art. 219 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, tj. Dz. U. z 2023 r., poz. 742, stopień doktora habilitowanego nadaje się osobie, która posiada stopień doktora oraz osiągnięcia naukowe, stanowiące znaczny wkład w rozwój określonej dyscypliny, jak również wykazuje się istotną aktywnością naukową realizowaną w więcej niż jednej uczelni, instytucji naukowej lub instytucji kultury.

Osiągnięcie naukowe może stanowić 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 ustawy Prawo o szkolnictwie wyższym i nauce. Warunek ten jest spełniony w przypadku cyklu powiązanych tematycznie artykułów naukowych pod tytułem: *Standardy prawne stosowania nieukierunkowanej inwigilacji elektronicznej przez organy władzy publicznej,* napisanych przez dra Marcina Rojszczaka. Artykuły są na wysokim poziomie naukowym i stanowią ważny wkład w rozwój dyscypliny nauki prawne.

Pozostały dorobek naukowy osiągnięty po uzyskaniu stopnia doktora także uzasadnia wniosek o nadanie Panu doktorowi Marcinowi Rojszczakowi stopnia naukowego doktora habilitowanego. Dorobek ten jest znaczący w zakresie osiągnięć naukowo-badawczych pod względem jakościowym i wystarczający pod względem ilościowym. Podobnie w obszarze dydaktycznym i popularyzatorskim osiągnięcia Habilitanta spełniają kryteria wskazane w przepisach.

Uwzględniając powyższe wnoszę o podjęcie dalszych czynności w celu nadania Panu doktorowi Marcinowi Rojszczakowi stopnia doktora habilitowanego.

M. Rogalski

Prof. dr hab. Maciej Rogalski