

Agnieszka Gryszczyńska

Katedra Prawa Informatycznego

Wydział Prawa i Administracji

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie

ul. Wóycickiego 1/3, p. 1756, 01-938 Warszawa

Załącznik nr 2

AUTOREFERAT

sporządzony dla celów postępowania habilitacyjnego, przedstawiający opis dorobku i osiągnięć naukowych oraz charakterystykę osiągnięcia naukowego w rozumieniu art. 16 ust. 2 ustawy z dnia 14 marca 2003 roku o stopniach naukowych i tytule naukowym oraz o stopniach i tytule naukowym w zakresie sztuki (t.j. Dz.U. z 2017 r., poz. 1789 ze zm.).

1. Imię i Nazwisko: Agnieszka Gryszczyńska

2. Posiadane dyplomy, stopnie naukowe – z podaniem nazwy, miejsca i roku ich uzyskania oraz tytuł rozprawy doktorskiej.

W maju 2005 roku ukończyłam z wynikiem bardzo dobrym jednolite studia magisterskie na kierunku prawo na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Uchwałą Rady Wydziału 47/2005/2006 przyznano mi dyplom z wyróżnieniem, otrzymałam również nagrodę Dziekana za najwyższą średnią. Pracę magisterską „Podpis elektroniczny w prawie polskim i włoskim na tle dyrektywy 1999/93/WE” napisałam pod kierunkiem prof. UKSW dr hab. Grażyny Szpor. W pracy magisterskiej zawarłam prawnoporównawcze badania dotyczące regulacji podpisów elektronicznych w Polsce i we Włoszech, które prowadziłam podczas studiów na Uniwersytecie w Cassino we Włoszech (Università degli Studi di Cassino e del Lazio Meridionale) w ramach stypendium z programu Erasmus (2004-2005 r.). Częściowo badania te zostały opublikowane w rozdziale „Oświadczenie woli opatrzone podpisem elektronicznym w Polsce oraz we Włoszech” w monografii „Prawo umów elektronicznych” pod redakcją J. Gołaczyńskiego (Zakamycze, Kraków 2006, s. 41-67) oraz w rozdziale “Application of electronic signatures in transferring the information about space w monografii “Geographic Information Systems in Research and Practice II nd Part” pod redakcją D. Kerekovića (Zagreb, 2005, s.138-142).

W tym samym roku ukończyłam również z wynikiem bardzo dobrym studia I stopnia na kierunku administracja. Uchwałą Rady Wydziału 47/2005/2006 przyznano mi dyplom z wyróżnieniem, otrzymałam również nagrodę Dziekana za najwyższą średnią. Pracę licencjacką ”Zastosowanie instrumentów elektronicznych w prawie zamówień publicznych” napisałam pod kierunkiem prof. UKSW dr hab. Grażyny Szpor.

Podczas studiów na Wydziale Prawa i Administracji UKSW uczęszczałam również na zajęcia prowadzone w ramach projektu badawczo-dydaktycznego Instytutu Politologii UKSW „Studium Generale Europa”, które ukończyłam uzyskując dyplom w 2005 roku.

Z uwagi na zainteresowania naukowe skoncentrowane na prawnych aspektach informatyzacji w latach 2003 - 2007 podjęłam studia na kierunku informatyka i ekonometria w Wyższej Szkole Ekologii i Zarządzania w Warszawie. Studia te ukończyłam z oceną bardzo dobrą, uzyskując tytuł zawodowy inżyniera. Pracę inżynierską pod tytułem „Informatyzacja ksiąg wieczystych w Polsce” napisałam pod kierunkiem dr Leszka Karskiego. Fragmenty pracy

inżynierskiej odnoszące się do aspektów prawnych informatyzacji zostały opublikowane jako rozdziały w monografiach: „Informatyzacja ksiąg wieczystych” [w:] Prawne problemy informatyzacji administracji, red. G. Szpor, Municipium S.A., Warszawa 2008, s. 81-88 oraz „Migracja ksiąg wieczystych” [w:] Elektroniczne aspekty wymiaru sprawiedliwości, red. G. Tylec, J. Misztal – Konecka, Oficyna Wydawnicza Branta, Bydgoszcz – Lublin 2009, s. 43-54.

W dniu 12. 04. 2011 r. uzyskałam stopień naukowy doktora nauk prawnych w zakresie prawa nadany uchwałą Rady Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, na podstawie rozprawy doktorskiej „Informatyzacja ksiąg wieczystych jako rejestru publicznego”. Promotorem rozprawy doktorskiej była prof. UKSW dr hab. Grażyna Szpor zaś recenzentami prof. UKSW dr hab. Małgorzata Jaśkowska oraz prof. dr hab. Zygmunt Niewiadomski.

Ponadto w latach 2005–2008 odbyłam aplikację prokuratorską, zakończoną egzaminem prokuratorskim.

3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych i pełnionych funkcjach

Od 1.10.2005 do 30.9.2011 roku zatrudniona byłam jako asystent w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Jako asystent prowadziłam ćwiczenia i konwersatoria na kierunkach prawo, administracja, stosunki międzynarodowe.

Od 2011 r. do chwili obecnej jestem zatrudniona jako adiunkt w Katedrze Prawa Informatycznego na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Jako adiunkt prowadziłam zajęcia na kierunkach prawo, administracja, stosunki międzynarodowe oraz człowiek w cyberprzestrzeni w formie wykładów, wykładów monograficznych, konwersatoriów, ćwiczeń oraz seminariów.

W dniu 30.9.2005 r. decyzją nr 36/2005 Dziekana Wydziału Prawa i Administracji UKSW zostałam powołana na stanowisko Pełnomocnika Dziekana ds. pozyskiwania środków pomocowych dla Wydziału Prawa i Administracji UKSW.

Ponadto od 2006 roku jestem wykładowcą studiów podyplomowych prowadzonych na Wydziale Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego

w Warszawie „Ochrona danych osobowych i informacji niejawnych”, a od 2018 r. również studiów podyplomowych „Ochrona danych osobowych w Kościele”. Od 2017 r. jestem wykładowcą „Studiów podyplomowych w zakresie rozpoznawania, zapobiegania i zwalczania cyberprzestępstw popełnianych na szkodę banków oraz ich klientów”, prowadzonych przez Wyższą Szkołę Policji w Szczytnie. Ponadto w 2019 r. przeprowadziłam wykłady na studiach podyplomowych „Ochrona danych osobowych” prowadzonych przez Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz „Ochrona danych osobowych” prowadzonych przez Akademię Leona Koźmińskiego w Warszawie. W 2017 r. byłam wykładowcą studiów podyplomowych „Zarządzanie bezpieczeństwem informacji”, prowadzonych przez Szkołę Główną Handlową.

Od 2017 r. jestem również wykładowcą Krajowej Szkoły Sądownictwa i Prokuratury, gdzie prowadzę zajęcia dla sędziów i prokuratorów z zakresu cyberprzestępczości. Byłam wykładowcą w ramach projektów „Szkolenia z zakresu prawa gospodarczego i cywilnego dla kluczowych kadr sądownictwa” oraz „Zapobieganie i zwalczanie cyberprzestępczości”.

Pracę naukowo – dydaktyczną łączę z pracą w prokuraturze, gdzie od 2016 r. specjalizuję się w zwalczaniu cyberprzestępczości. Od 12.7.2018 r. jestem koordynatorem postępowań z zakresu cyberprzestępczości w Wydziale I do Spraw Przestępczości Gospodarczej Prokuratury Regionalnej w Warszawie, zaś w okresie od 23.09.2016 r. do 10.7.2018 r. pełniłam funkcję kierownika Działu III (zwalczania cyberprzestępczości) w Wydziale II Śledczym, a następnie w Wydziale II do Spraw Przestępczości Gospodarczej Prokuratury Okręgowej w Warszawie.

Od 19.2.2019 r. jestem członkiem Rady do Spraw Cyfryzacji.

4. **Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki, tj. Dz.U. z 2017 r., poz. 1789 ze zm.**

4.1. Wskazanie osiągnięcia naukowego

Jako osiągnięcie naukowe w dyscyplinie naukowej prawo, spełniające wymogi wskazane w art. 16 ust. 1 i ust. 2 pkt. 1 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki, tj. Dz.U. z 2017 r., poz. 1789 ze zm., wskazuję cykl publikacji powiązanych tematycznie „**Jawność i bezpieczeństwo rejestrów publicznych**”. Cykl składa się z 11 publikacji stanowiących rozdziały w recenzowanych monografiach i obejmuje ok. 24 arkuszy wydawniczych [około 540 stron znormalizowanych]. Publikacje wchodzące w skład cyklu zostały wydane w okresie od 2013 r. do 2017 r. W przeważającej części rozdziały te stanowią efekt badań prowadzonych przeze mnie w okresie od 9.5.2013 r. do 9.7.2016 r. w ramach projektu badawczo-rozwojowego realizowanego na rzecz bezpieczeństwa i obronności państwa „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym”, DOBR/0075/R/ID2/2013/03, współfinansowanego ze środków NCBiR (zwanego dalej projektem MRJ), gdzie koordynowałam zadanie „Analiza polskiej regulacji ograniczeń jawności oraz powiązanych z nimi aktów prawa europejskiego i międzynarodowego” oraz byłam wykonawcą w zadaniu „Weryfikacja regulacji jawności i ograniczeń jawności publicznych zasobów informacyjnych. Racjonalne wykorzystanie interoperacyjności elektronicznych rejestrów publicznych i zbiorów poza rejestrowych, informacji o prawie i dostępie do akt”.

Cykl tworzą następujące publikacje:

1. A. Gryszczyńska, **Pojęcie i jawność rejestrów publicznych - uwagi wprowadzające**, w: Rejestry publiczne. Jawność i interoperacyjność, red. A. Gryszczyńska, C.H. Beck, Warszawa 2016, s. 3-39, ISBN: 9788325586843 (recenzent wydawniczy: prof. US, dr hab. Aleksandra Monarcha-Matlak);
2. A. Gryszczyńska, **Podstawy prawne ograniczeń jawności w Polsce**, w: A. Gryszczyńska (red.), Struktura tajemnic, Tom VI monografii Jawność i jej ograniczenia, G. Szpor (red.), C.H.Beck, Warszawa 2016 (wydanie II), s. 1-49, ISBN: 978-83-255-8818-2 (recenzent wydawniczy: prof. UW, dr hab. Jerzy Korczak);
3. A. Gryszczyńska, **Struktura regulacji tajemnic ustawowo chronionych**, w: A. Gryszczyńska (red.), Struktura tajemnic, Tom VI monografii Jawność i jej ograniczenia,

- G. Szpor (red.), C.H.Beck, Warszawa 2016 (wydanie II), s. 273-327, ISBN: 978-83-255-8818-2 (recenzent wydawniczy: prof. UW, dr hab. Jerzy Korczak);
4. A. Gryszczyńska, **Jawność formalna ksiąg wieczystych w Polsce**, w: Rejestry publiczne. Jawność i interoperacyjność, red. A. Gryszczyńska, C.H.Beck, Warszawa 2016, s. 255-310, ISBN: 9788325586843 (recenzent wydawniczy: prof. US dr hab. Aleksandra Monarcha-Matlak);
 5. A. Gryszczyńska, **Jawność formalna rejestru zastawów**, w: Rejestry publiczne. Jawność i interoperacyjność, red. A. Gryszczyńska, C.H. Beck, Warszawa 2016, s. 335-350, ISBN: 9788325586843 (recenzent wydawniczy: prof. US, dr hab. Aleksandra Monarcha-Matlak);
 6. A. Gryszczyńska, **Jawność formalna ewidencji partii politycznych**, w: Rejestry publiczne. Jawność i interoperacyjność, red. A. Gryszczyńska, C.H. Beck, Warszawa 2016, s. 367-382, ISBN: 9788325586843 (recenzent wydawniczy: prof. US, dr hab. Aleksandra Monarcha-Matlak);
 7. G. Szpor, M. Durzyńska, A. Gryszczyńska, I. Kamińska, K. Mączewski, W. Radzio, Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne. Komentarz, Warszawa 2013, **w zakresie komentarzy do artykułów mojego autorstwa, gdzie analizie poddałam podstawy prawne ewidencjonowania danych przestrzennych w katastrze nieruchomości, funkcje tego rejestru, zakres danych podlegających wpisowi oraz zakres jawności**, to jest: art. 20 (nb. 1-4, 6, 8, 9,10), art. 21 (nb. 2, 3, 5, 6, 7, 8, 9), art. 23, art. 24, art. 25 (nb. 1, 2, 4), art. 40 a, art. 48), strony: 169-179, 189-190, 194-199, 200-210, 215-249, 259-260, 262-263, 436-439, 517-526, ISBN: 978-83-278-006-0;
 8. A. Gryszczyńska, **Legal limitations of public access to spatial data in Poland [Prawne ograniczenia publicznego dostępu do danych przestrzennych]**, w: Access to spatial data and its limitations. Legal aspects, red. G. Szpor, A. Gryszczyńska, wydawca Croatian Information Technology Society, GIS Forum, Naukowe Centrum Prawno-Informatyczne, Zagreb 2015 r., s. 50-67, ISBN 978-953-6129-52-2 Nacionalna knjižnica, Zagreb, Croatia (recenzent wydawniczy: Tihomir Katulić, Phd, LL.M; Information Technology Law Department, Faculty of Law, University of Zagreb, Croatia);
 9. A. Gryszczyńska, **Cybersecurity of public registers in Poland: selected legal issues [Cyberbezpieczeństwo rejestrów publicznych w Polsce: wybrane uwarunkowania prawne]**, w: Geographic Information Systems Conference and Exhibition “GIS

Odyssey2016”- Conference proceedings, red. A. Bieda, J. Bydłosz, A. Kowalczyk, Zagreb 2016, s. 105-113, ISBN 978-953-6129-55-3 (Nacionalna knjižnica, Zagreb, Croatia), publikacja indeksowana w bazie Web of Science;

10. A. Gryszczyńska, **Nowe zagrożenia bezpieczeństwa rejestrów publicznych**, w: Internet. Strategie bezpieczeństwa, red. G. Szpor, A. Gryszczyńska, C.H. Beck, Warszawa 2017, s. 293-309, ISBN: 978-83-255-9700-9 (recenzent wydawniczy: prof. UKSW, dr hab. Bogumił Szmulik);
11. A. Gryszczyńska, **Postulaty zmian w zakresie jawności i bezpieczeństwa rejestrów publicznych**; w: T. Bąkowski (red.) Model regulacji, Tom XII monografii Jawność i jej ograniczenia, G. Szpor (red.), C.H. Beck, Warszawa 2016, s. 181-198, ISBN: 978-83-255-9452-7 (recenzent wydawniczy: prof. UKSW, dr hab. Zbigniew Cieślak).

4.2. Omówienie celu naukowego

Dobór tematu cyklu naukowego zgodny jest z moim zainteresowaniami naukowymi. Od kilkunastu lat prowadzę badania nad wpływem informatyzacji na realizację zadań publicznych. Moje zainteresowania ogniskują się na prawnych, organizacyjnych i technicznych problemach prowadzenia rejestrów publicznych oraz udostępniania danych w nich zawartych. Aktywność w tym obszarze przejawiałam jeszcze przed uzyskaniem stopnia doktora nauk prawnych, przy czym koncentrowałam się wówczas głównie na procesie informatyzacji rejestrów sądowych i zasobów geoinformacyjnych (A. Gryszczyńska, Dostęp do danych osobowych z rejestrów sądowych [w:] Ochrona danych osobowych. Skuteczność regulacji, red. G. Szpor, Municipium S.A., Warszawa 2009, s. 145-164, A. Gryszczyńska, Access to information on legal status of real estates in Poland [w:] Time, GIS & Future, red. D. Kereković, GIS Forum, Zagreb 2009, s. 251-257, A. Gryszczyńska, Migracja ksiąg wieczystych [w:] Elektroniczne aspekty wymiaru sprawiedliwości, red. G. Tylec, J. Misztal – Konecka, Oficyna Wydawnicza Branta, Bydgoszcz – Lublin 2009, s. 43-54, A. Gryszczyńska, Informatyzacja ksiąg wieczystych [w:] Prawne problemy informatyzacji administracji, red. G. Szpor, Municipium S.A., Warszawa 2008, s. 81-88, A. Gryszczyńska, Geoinformation in real estate and mortgage register [w:] Geoinformation challenges, red. M. Gajos, M. Styblińska, Wydawnictwo Uniwersytetu Śląskiego, Sosnowiec 2008, s. 71-78, A. Gryszczyńska, B. Konieczna, The migration of data from paper real estate and mortgage registers to electronic ones [w:] Richness and Diversity of GIS, red. D. Kereković, GIS Forum, Zagreb 2007, s. 166-174, A. Gryszczyńska, B. Konieczna, New Land Register System in Poland [w:] GIS Applications and Development, red. D. Kereković, GIS Forum, Zagreb 2006, s. 142-148,

A. Gryszczyńska, Application of electronic signatures in transferring the information about space [w:] Geographic Information Systems in Research and Practice II nd Part, red. D. Kereković, Zagreb, 2005, s.138-142).

Badania nad jawnością i bezpieczeństwem rejestrów publicznych stanowią również kontynuację rozważań podjętych przeze mnie w dysertacji doktorskiej „Informatyzacja ksiąg wieczystych jako rejestru publicznego”, w której poddałam weryfikacji ogólną tezę, według której informatyzacja wymusza reorientację funkcji rejestru, pojmowanych według socjologii administracji, jako zorientowane na określony cel działania normatywnie postulowane i realnie obserwowane. Przyjęłam wówczas, że cele ksiąg wieczystych -rozumiane jako wartości, dla których urzeczywistnienia i ochrony ustanowiono instytucję prawną - pozostają stałe, natomiast w wyniku informatyzacji znaczącej zmianie ulegają operacje normatywnie postulowane dla realizacji założonych celów, czyli zadania związane z prowadzeniem ksiąg wieczystych. Problematyka ta była również przeze mnie podejmowana po uzyskaniu stopnia naukowego doktora nauk prawnych w zakresie prawa (m.in. w pracach: A. Gryszczyńska, Nowa Księga Wieczysta. Informatyzacja rejestru publicznego, 423 s., LexisNexis, Warszawa 2011 stanowiącej zaktualizowaną i zmodyfikowaną wersję rozprawy doktorskiej, A. Gryszczyńska, Elektroniczny dostęp do Nowej Księgi Wieczystej i Krajowego Rejestru Sądowego [w:] Internet. Prawno-informatyczne problemy sieci, portali i e-usług, red. G. Szpor i W.R. Wiewiórowski, Wyd. C.H.Beck, Warszawa 2012, s. 289-303).

Instytucja rejestrów publicznych stanowi zarówno istotne- choć nie do końca zbadane - zagadnienie prawne, jak i problem techniczno-organizacyjny. W piśmiennictwie prawniczym dominują opracowania dotyczące poszczególnych rejestrów publicznych, do wyjątków należą kompleksowe analizy poświęcone tej instytucji¹. Badania dotyczące rejestrów publicznych, jak również procesów ich informatyzacji wymagają interdyscyplinarnego spojrzenia. Problematyka rejestrów publicznych oraz ich informatyzacji obejmując zagadnienia materialnoprawne, proceduralne i ustrojowe, jest głównie domeną prawa publicznego. Rejestry i ewidencje zostały uznane w „Systemie Prawa Administracyjnego” za jedną z podstawowych instytucji materialnego prawa administracyjnego. Problematyka wpisów do rejestrów publicznych w funkcjonowaniu norm prawa administracyjnego była przedmiotem analizy Jacka Jagielskiego, który wskazał, że zagadnienie wpisów do rejestrów stanowi płaszczyznę badawczą nową i nietypową. Konstatując tendencję ustrojową lawinowego tworzenia przez prawodawcę rejestrów wyznaczył on nowe kierunki badawcze w obszarze prawa

¹ T. Stawecki, Rejestry publiczne. Funkcje instytucji, Warszawa 2005; J. Oleński, Infrastruktura informacyjna państwa w globalnej gospodarce, Warszawa 2006.

administracyjnego materialnego, którymi są cele, sposoby organizacji i funkcjonowania rejestrów, a także odpowiedź na pytanie czy rozprzestrzenianie się rejestrów i innych urzędowych wykazów, nie niesie za sobą nowej płaszczyzny ingerencji władzy publicznej w sferę praw jednostek. Pozwala to uznać, że problematyka rejestrów publicznych, nie tylko w kontekście instytucji prawa administracyjnego materialnego, stanowi pole dla szerokiej, pogłębionej penetracji badawczej².

Badania dotyczące jawności i bezpieczeństwa rejestrów publicznych w Polsce wskazują, że rozwój technicznej interoperacyjności rejestrów publicznych, znoszenie barier technicznych i organizacyjnych udostępniania danych powiązane z wykorzystywaniem do prowadzenia rejestrów systemów teleinformatycznych, oddziałują na realizację zadań publicznych, dostępność elektronicznych usług publicznych oraz jakość i spójność danych. Informatyzacji, integracji i elektronicznemu udostępnianiu danych rejestrowych towarzyszą jednak nieznane dotąd zagrożenia związane z agregacją, analizą i wykorzystaniem danych przy zastosowaniu metod *big data* charakteryzujących się łatwością łączenia danych ze zbiorów wielkoskalowych z nowymi zasobami i nieznanymi w momencie, gdy został zdefiniowany pierwotny cel i sposoby przetwarzania danych sposobami ich eksploracji. Nowe zagrożenia wiążą się również z rozwojem cyberprzestępczości i incydentami, które mogą objąć rejestry publiczne i utrudnić lub uniemożliwić realizację zadań publicznych, opartych w dużej mierze na dostępie do zasobów informacyjnych. Skłania to do poszukiwania optymalnego modelu udostępniania danych, który zapewni realizację celów rejestru przy jednoczesnej minimalizacji zagrożeń zarówno dla prywatności podmiotów podlegających wpisowi, jak i bezpieczeństwa publicznego.

Z uwagi na doniosłość problematyki jawności i bezpieczeństwa rejestrów publicznych, w badaniach jawności i jej ograniczeń prowadzonych w projekcie Model Regulacji Jawności uwzględniono oraz poddano analizie regulacje normatywne dostępu do danych z wybranych rejestrów. Badania nad instytucją utrudnia jednak mnogość rejestrów, aktów prawnych, na podstawie których są prowadzone, różnorodność celów rejestrów, funkcji przez nie pełnionych, gromadzonych danych i zasad dostępu do nich, a także odmienny stopień ich informatyzacji. Rozproszona i niespójna regulacja odnosząca się do udostępniania informacji

² J. Jagielski, Wpisy do rejestrów, ewidencji i innych urzędowych wykazów [w:] Prawo administracyjne materialne. System Prawa Administracyjnego tom 7, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2017, s. 481-503.

z kilkuset rejestrów publicznych³, pozostaje dodatkowo w niejasnych relacjach z przepisami odnoszącymi się do ochrony tajemnic, dostępu do informacji publicznej, ponownego wykorzystywania informacji sektora publicznego oraz ochrony danych osobowych. Ustalenia w tym zakresie mogą stanowić, jak wskazuje Grażyna Szpor, częściowe wypełnienie postulatu eksploracji problematyki rejestrów publicznych i jednocześnie podstawę do ponownego rozważenia skutków wpisów o charakterze informacyjnym⁴.

Celem cyklu **„Jawność i bezpieczeństwo rejestrów publicznych”** jest analiza związanych z informatyzacją zmian zasad i zakresu udostępniania danych z wybranych rejestrów publicznych, przy uwzględnieniu celu prowadzenia rejestru, jego funkcji oraz dóbr i wartości chronionych, prowadzona w oparciu o rozważania nad regulacją prawną jawności i jej ograniczeń w demokratycznym państwie prawnym.

Weryfikacji poddano tezę, że postulowana w związku z informatyzacją i elektronicznym udostępnianiem danych rejestrowych redefinicja tradycyjnie pojmowanej jawności formalnej rejestru, powinna obecnie uwzględniać nowe możliwości agregacji i analizy danych związane z postępem technicznym w drugiej dekadzie XXI wieku, nasilające zagrożenia praw i wolności człowieka oraz interesu publicznego. Weryfikacja hipotezy o nadmiarowości, niespójności i braku elastyczności przepisów regulujących ograniczenia jawności, może być podstawą postulatów *de lege ferenda* zorientowanych na ochronę cyberbezpieczeństwa.

Cykl publikacji otwiera rozdział monografii „Rejestry publiczne. Jawność i interoperacyjność”, w której akcent położono na dwa zagadnienia związane z prowadzeniem rejestrów publicznych – dostęp do danych zgromadzonych w rejestrze (jawność formalną) oraz interoperacyjność. Wybór problemów i próby badawczej podyktowany był koniecznością uwzględnienia aktualnych problemów prowadzenia rejestrów wynikających z cyfryzacji zasobów informacyjnych i stosowania środków komunikacji elektronicznej. W pierwszym rozdziale **„Pojęcie i jawność rejestrów publicznych - uwagi wprowadzające”** poddałam analizie pojęcie rejestru publicznego w oparciu o definicję legalną rejestru publicznego, wprowadzoną do prawa polskiego ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2019 r. poz. 700) oraz definicje doktrynalne (w tym w szczególności definicje sformułowane w monografiach Tomasza Staweckiego i Józefa

³ Wskazuje się, że w bazie wiedzy prowadzonej przez GUS zgromadzono szczegółowe opisy 587 rejestrów (J. Dygaszewicz, Problemy i perspektywy związane z funkcjonowaniem rejestrów publicznych [w:] Rejestry publiczne. Jawność i interoperacyjność, A. Gryszczyńska (red.), Warszawa 2016, s. 109).

⁴ G. Szpor, Jurystyka jawności i jej ograniczeń w XXI wieku, w: G. Szpor, Jawność i jej ograniczenia, t. I, Idee i pojęcia, Warszawa 2016, s. 193.

Oleńskiego). Definicje te zostały zestawione z definicjami rejestru urzędowego oraz systemów informacyjnych administracji publicznej określonymi w ustawie o statystyce publicznej (t.j. Dz.U. z 2019 r. poz. 649). Dokonane ustalenia terminologiczne mają istotne znaczenie dla określenia zakresu obowiązków organu rejestrowego wynikających z ustaw o informatyzacji, statystyce czy dostępie do informacji publicznej (t.j. Dz.U. z 2018 r. poz. 1330 ze zm.), zwłaszcza, że chaos terminologiczny powoduje trudności interpretacyjne związane z zaliczeniem danego zbioru do kategorii rejestrów publicznych⁵. Na tle analizowanych definicji rejestru publicznego analizie poddałam związek między „publicznością” a „jawnością” rejestru. Dalsze rozważania poświęcone są omówieniu funkcji rejestrów, w tym kluczowej z perspektywy badań nad jawnością rejestrów funkcji informacyjnej.

Samo pojęcie jawności w doktrynie prawa definiowane jest różnie w zależności od celu prowadzonych badań – jako idea⁶, wartość⁷, zasada⁸, jako postulat, opis działań czy stan faktyczny⁹. Pojęcie to było przy tym przedmiotem pogłębionych badań, rozważania podjęte w tym rozdziale skoncentrowałam zatem na jawności formalnej rejestrów oraz podstawach prawnych udostępniania danych rejestrowych, opierając się na ustaleniach dotyczących pojęcia jawności projektu MRJ¹⁰.

⁵ G. Szpor, Problemy informatyzacji rejestrów sądowych, Gdańskie Studia Prawnicze - Przegląd Orzecznictwa, 2015, nr 4, s. 33 i n.

⁶ A. Piskorz-Ryń, Ocena dopuszczalnych ograniczeń jawności ze względu na wymagania konstytucyjne, w: G. Szpor (red.), Jawność i jej ograniczenia, t. III Skuteczność regulacji, Z. Kmiecik (red.), Warszawa 2013, s. 43.

⁷ T. Stawecki, Jawność jako wartość prawna, Studia Iuridica 2004, nr 43, s. 221; A. Dylus, Aksjologiczne podstawy jawności i jej ograniczenia. Perspektywa etyki politycznej, w: Jawność i jej ograniczenia G. Szpor (red.), t. II Podstawy aksjologiczne. Z. Cieślak (red.), Warszawa 2013, s. 16; T. Górzyńska, Prawo do informacji i zasada jawności administracyjnej, Kraków 1999, s. 27–28; J. Zimmermann, Prawo administracyjne, Warszawa 2014, s. 124–125.

⁸ J. Karczewski, T. Stawecki, Jawność i prywatność – ważenie zasad prawnych, w: A. Mednis (red.), Prywatność a jawność. Bilans 25 - lecia i perspektywy na przyszłość, Warszawa 2016, s. 127 i n.; J. Zajadło, Zasada jawności a filozoficzne pojęcie prawdy, w: Jawność i jej ograniczenia, G. Szpor (red.), t. II Podstawy aksjologiczne, Z. Cieślak (red.), Warszawa 2013, s. 53.

⁹ Z. Cieślak, Podstawy aksjologiczne jawności i ograniczeń jawności – synteza, w: Jawność i jej ograniczenia, G. Szpor (red.), t. II Podstawy aksjologiczne, Z. Cieślak (red.), Warszawa 2013, s. 131–132.

¹⁰ G. Szpor, Jurydyzacja jawności i jej ograniczeń w XXI wieku, s. 1-79; G. Szpor, Znaczenie terminologii w badaniach jawności i jej ograniczeń, w: G. Szpor Jawność i jej ograniczenia, t. I, Idee i pojęcia, Warszawa 2016, s. 81-165; Z. Cieślak, Podstawy aksjologiczne jawności i ograniczeń jawności – synteza, s. 131–132; Dylus, Aksjologiczne podstawy jawności i jej ograniczenia. Perspektywa etyki politycznej, s. 16; A. Gryszczyńska, Podstawy prawne ograniczeń jawności w Polsce, w: G. Szpor (red.), Jawność i jej ograniczenia, t. VI Struktura tajemnic, A. Gryszczyńska (red.), Warszawa 2014, s. 3 -6; A. Piskorz-Ryń, Ocena dopuszczalnych ograniczeń jawności ze względu na wymagania konstytucyjne, s. 43; A. Piskorz-Ryń, Jawność i ograniczenia jawności publicznych zasobów informacyjnych, w: G. Szpor (red.), Jawność i jej ograniczenia, t. V Dostęp i wykorzystanie, A. Piskorz-Ryń (red.), s. 5–16; T. Jaroszyński, Analiza pojmowania i działania zasady jawności oraz jej ograniczeń z perspektywy prawa włoskiego, w: G. Szpor (red.), Jawność i jej ograniczenia, t. XI, Standardy europejskie C. Mik (red.), Warszawa 2016, s. 213–214; K. Doktor-Bindas, Analiza pojmowania i działania zasady jawności oraz jej ograniczeń z perspektywy prawa włoskiego, w: G. Szpor (red.), Jawność i jej ograniczenia, t. XI Standardy europejskie C. Mik (red.), Warszawa 2016, s. 179–183; T. Chauvin, Analiza pojmowania i działania zasady

Dostęp do danych rejestrowych może być ograniczony koniecznością wykazania przez wnioskującego interesu, dane te mogą również stanowić tajemnice. Z badaniami nad jawnością rejestrów publicznych ściśle powiązana jest analiza ograniczeń jawności, zawarta w rozdziale **„Podstawy prawne ograniczeń jawności w Polsce”** opublikowanym w tomie VI monografii **„Jawność i jej ograniczenia. Struktura tajemnic”**, w której zawarto ustalenia dokonane w ramach koordynowanego przeze mnie zadania "Analiza polskiej regulacji ograniczeń jawności oraz powiązanych z nimi aktów prawa europejskiego i międzynarodowego". Celem badań było dokonanie kompleksowego przeglądu przepisów prawnych odnoszących się do realizacji zasady jawności i jej ograniczeń oraz weryfikacja hipotezy o nadmiarowości regulacji ograniczeń jawności oraz niespójności przepisów w tym zakresie. Analizie poddano akty prawne konstytuujące tajemnice prawnie chronione oraz wprowadzające inne ograniczenia w dostępie do informacji. Ponieważ na stan faktycznej jawności wpływ mogą wywierać również czynniki organizacyjne czy techniczne determinujące sposób udostępniania danych (czas oczekiwania, miejsce dostępu, koszty, przyjęte kryteria wyszukiwawcze) na przykładzie rejestrów sądowych, cechujących się szeroką jawnością formalną weryfikowano w jaki sposób organizacja i stan informatyzacji danego zbioru determinuje dostępność danych rejestrowych i potwierdzono, że istotny wpływ na funkcję informacyjną wywiera technika prowadzenia rejestru.

Sposób regulacji ograniczeń jawności spełniających materialne i formalne przesłanki wyodrębnienia tajemnic był przedmiotem analiz zawartych w rozdziale **„Struktura regulacji tajemnic ustawowo chronionych”** opublikowanym w tomie VI monografii **„Jawność i jej ograniczenia. Struktura tajemnic”**. Ponieważ tajemnice będące ograniczeniem wolności informacyjnej i prawa dostępu do informacji publicznej mogą zostać ustanowione wyłącznie wówczas, gdy wprowadzenie poufności znajduje uzasadnienie w katalogu chronionych konstytucyjnie wartości, analizie poddałam wartości wskazane w art. 31 ust. 3 oraz art. 61 ust. 3 Konstytucji RP. Z uwagi na to, że określone w Konstytucji RP pole aksjologicznych wyborów podlega uszczegółowieniu w aktach normatywnych niższego rzędu, w dalszej części rozważań poszukiwałam odniesienia do wartości, dla których ustanowiono ochronę określonych informacji w ustawach wprowadzających tajemnicę. Analizie poddałam pojęcie tajemnicy, sposoby wprowadzania obowiązku zachowania tajemnicy, sposób regulacji zakresu przedmiotowego tajemnic, podmiotów zobowiązanych do zachowania tajemnic i ich

jawności oraz jej ograniczeń z perspektywy prawa francuskiego, w: G. Szpor (red.), *Jawność i jej ograniczenia*, t. XI, Standardy europejskie C. Mik (red.), Warszawa 2016, s. 134–135.

obowiązków, podmiotów chronionych tajemnicą i ich uprawnień, okresu utajnienia. Badałam również przejawianie się elementu formalnego.

Po przeprowadzeniu aksjologicznych rozważań odnoszących się do jawności i jej ograniczeń, uwzględniając różny zakres i sposoby urzeczywistniania formalnej jawności, dokonałam analizy rozwiązań przyjętych dla wybranych rejestrów publicznych. Rozważałam w szczególności czy normatywne określenie "rejestr jest jawny" oznacza prawo każdego do dostępu do wszystkich zgromadzonych danych, prawo do wyszukiwania danych w zbiorze na podstawie zróżnicowanych kryteriów, podstawę do udostępnienia w Internecie danych rejestrowych czy też prawo do ponownego wykorzystania danych rejestrowych. Uwzględnione zostały przy tym zmiany wywołane informatyzacją - zarówno jeśli chodzi o zmiany techniczno-organizacyjne prowadzenia rejestrów, jak i towarzyszące informatyzacji zmiany przepisów prawnych, poszerzające krąg podmiotów uprawnionych do uzyskania odpisów czy wprowadzające nowe usługi w zakresie udostępniania i wyszukiwania informacji. Z uwagi na wiążące się z udostępnianiem w Internecie publicznych zasobów informacyjnych, przesuwanie się granic między jawnością a ochroną innych dóbr pozostających w kolizji z jawnością (w tym zwłaszcza prywatności), zjawiska te nie zawsze oceniać należy pozytywnie.

Prowadzone przeze mnie badania dotyczące jawności formalnej wybranych rejestrów zostały opublikowane w rozdziałach **„Jawność formalna ksiąg wieczystych w Polsce”, „Jawność formalna rejestru zastawów”, „Jawność formalna ewidencji partii politycznych”** monografii **„Rejestry publiczne. Jawność i interoperacyjność”**. Przyjętą perspektywę badawczą poszerzały badania przeprowadzone przez innych autorów rozdziałów tej monografii, stanowiąc bazę dla formułowania wniosków ogólnych. Ponadto ustalenia dotyczące jawności ewidencji gruntów i budynków zawarłam w **komentarzu do ustawy z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne** mojego współautorstwa oraz w rozdziale **„Legal limitations of public access to spatial data in Poland”** [Prawne ograniczenia publicznego dostępu do danych przestrzennych] opublikowanym w monografii **„Access to spatial data and its limitations. Legal aspects”** pod moją współredakcją.

Zabezpieczenie rejestrów publicznych przed atakami z cyberprzestrzeni dopiero od niedawna stało się przedmiotem dyskusji naukowej i działań podejmowanych przez podmioty publiczne. Zmiana techniki przetwarzania wpływająca na urzeczywistnienie formalnej jawności rejestrów, udostępnianie zasobów on-line oraz pojawianie się nowych możliwości eksploracji i wykorzystania danych (w tym metod *Big Data*, dzięki którym możliwe jest zastosowanie zróżnicowanych sieci i strategii "połowu danych" z "oceanu danych") sprawiają,

że publiczne zasoby informacyjne stanowią obiekt zainteresowania ze strony grup przestępczych czy wywiadów obcych państw.

W rozdziale pod tytułem „**Cybersecurity of public registers in Poland: selected legal issues [Cyberbezpieczeństwo rejestrów publicznych w Polsce: wybrane uwarunkowania prawne]**” opublikowanym w monografii „Geographic Information Systems Conference and Exhibition. GIS Odyssey 2016” pod redakcją Agnieszki Biedy, Jarosława Bydłosza i Anny Kowalczyk, analizie poddałam wybrane problemy zapewnienia cyberbezpieczeństwa rejestrów w Polsce - związane z elektronicznym udostępnianiem danych rejestrowych, brakiem interoperacyjności czy ustawowego wskazania podmiotów odpowiedzialnych za system teleinformatyczny obsługujący rejestr i zapewnienie bezpieczeństwa danych rejestrowych. Nowe zagrożenia związane m.in. z nieuprawnionym pozyskaniem i wykorzystaniem danych rejestrowych przez przestępców, atakami zagrażającymi integralności danych, czy ich dostępności, uczyniłam przedmiotem rozważań zawartych w rozdziale „**Nowe zagrożenia bezpieczeństwa rejestrów publicznych**”, opublikowanym w monografii „Internet. Strategie bezpieczeństwa”, w którym skupiłam się na zagrożeniach związanych ze zmianami zasad udostępniania danych rejestrowych zarówno podmiotom realizującym zadania publiczne jak również podmiotom prywatnym, a także na konsekwencjach braku wystarczających mechanizmów kontroli elektronicznego dostępu do rejestrów i adekwatnych do naruszeń sankcji. Rozważania te mogą stać się punktem wyjścia dla opracowania rozwiązań prawnych i organizacyjnych zwiększających bezpieczeństwo rejestrów.

Podsumowanie badań koncentrujących się wokół zasad elektronicznego udostępniania danych oraz analizy zagrożeń związanych z wykorzystaniem systemów teleinformatycznych do prowadzenia rejestrów publicznych, zawarłam w rozdziale „**Postulaty zmian w zakresie jawności i bezpieczeństwa rejestrów publicznych**” opublikowanym w tomie XII monografii „Jawność i jej ograniczenia. Model regulacji” pod redakcją Tomasza Bąkowskiego. W rozdziale tym sformułowałam najistotniejsze postulaty dotyczące jawności formalnej i bezpieczeństwa rejestrów publicznych. Mogą one stać się punktem wyjścia dla prac legislacyjnych mających na celu systemowe uregulowanie zasad dostępu do rejestrów publicznych, zdefiniowanie zadań publicznych związanych z prowadzeniem rejestrów publicznych, a także stworzenie rozwiązań prawnych i organizacyjnych zwiększających bezpieczeństwo rejestrów.

Osiągnięciu postawionych celów badań służą wybrane metody badawcze. Dla realizacji badań nad regulacją jawności i bezpieczeństwa rejestrów publicznych podstawowe znaczenie miała metoda dogmatyczna. Metodę porównawczą zastosowano w badaniach struktury

tajemnic oraz ochrony publicznych zasobów informacyjnych. Ukazanie ewolucji regulacji jawności, wymagało zastosowania metody historycznej. Była ona pomocna w ustaleniu zmian dokonujących się w regulacji prawnej jawności formalnej rejestrów, związanej ze zmianami techniki prowadzenia zasobów. Sformułowanie określonych wniosków wymagało również sięgnięcia do dorobku doktryny i judykatury.

4.3. Omówienie osiągniętych wyników oraz postulatów zmian

Rozważania dotyczące istotnych elementów definicyjnych pojęcia rejestru publicznego prowadzą do wniosku, że dla uznania zasobu za rejestr publiczny konieczne jest spełnienie trzech przesłanek: 1) zasób ma być prowadzony na podstawie przepisów ustawowych; 2) podmiotem prowadzącym ma być podmiot publiczny; 3) zasób ten ma służyć do realizacji zadań publicznych. Pojęciem szerszym od pojęcia rejestru publicznego jest pojęcie rejestru urzędowego określone w ustawie o statystyce publicznej, albowiem w definicji rejestru urzędowego mieszczą się również zasoby, które nie są prowadzone przez podmiot publiczny, nie muszą służyć do realizacji zadań publicznych, a podstawą ich prowadzenia mogą być również akty wykonawcze. Analiza definicji normatywnych prowadzi przy tym do jednoznacznej konstatacji, że ustawodawca konstruując pojęcie rejestru publicznego i rejestru urzędowego, nie zaliczył do ich elementów konstrukcyjnych jawności. W definicji rejestru publicznego mieścić się będą również te zasoby, do których dostęp został ograniczony, o ile zasób ten jest prowadzony przez podmiot publiczny na podstawie przepisów ustawowych i służy do realizacji zadań publicznych. Analiza definicji rejestru wskazuje również, że za rejestry publiczne, o ile spełniają powyższe cechy, mogłyby być uznane również zasoby, do których dostęp przysługuje jedynie podmiotom publicznym (wewnętrzne zasoby informacyjne). „Publiczność” rejestru aktualnie interpretować należy zatem w odniesieniu do celu jego ustanowienia – to jest realizacji zadań publicznych oraz podmiotu prowadzącego rejestr będącego podmiotem publicznym (szerzej m.in. w: Pojęcie i jawność rejestrów publicznych - uwagi wprowadzające, s. 9-17, Jawność formalna ksiąg wieczystych w Polsce, s. 293-307).

W dalszych rozważaniach określiłam determinanty jawności zasobów rejestrowych. Badania nad ograniczeniami jawności rozpoczęłam od analizy ogólnych warunków dopuszczalności ustanawiania ograniczeń jawności określonych w Konstytucji, w której wskazano jako kryteria oceny dopuszczalności ograniczeń praw i wolności – zasadę wyłączności ustawy, zasadę proporcjonalności oraz obowiązek poszanowania istoty praw i wolności. Ograniczenia dostępu do informacji wprowadzone mogą być ponadto jedynie pod

warunkiem ich konieczności dla realizacji określonych konstytucyjnie wartości (szerzej w: Podstawy prawne ograniczeń jawności w Polsce, s. 1-49).

Następnie analizie poddałam ograniczenia jawności stanowiące tajemnice. Przeprowadzone badania wykazały, że ustawodawca wprowadza ograniczenia jawności w postaci tajemnic w różny sposób – poprzez jednoznaczne wskazanie istnienia tajemnicy oraz podanie jej jurydycznej nazwy, poprzez mniej lub bardziej wyraźne określenie materialnych i formalnych przesłanek tajemnic, po regulacje, w których wątpliwości budzi charakter wprowadzanego ograniczenia jawności. Punktem wyjścia do badań nad strukturą tajemnic uczyniłam więc analizę sposobów wprowadzania obowiązku zachowania tajemnicy. Takie kryterium powinno pozwolić również dekodować materialne i formalne przesłanki tajemnic oraz kształtować pożądany model regulacji.

Dokonana analiza aktów prawnych odnoszących się do tajemnic ustawowo chronionych, wskazuje na rozproszenie i niejednorodność regulacji. Jedynie część z przepisów odwołujących się do obowiązku zachowania tajemnicy pozwoliła zrekonstruować materialne i formalne przesłanki wskazujące na istnienie tajemnicy ustawowo chronionej. Przeprowadzone badania potwierdziły przy tym tezę o nadmiarowości, niejednorodności i niespójności przepisów dotyczących tajemnic. Nadregulacja związana jest w szczególności z niekonsekwentnie stosowaną przez ustawodawcę terminologią, wprowadzaniem nowych tajemnic mających na celu ochronę tych samych wartości, a także z wprowadzaniem odrębności w ochronie określonych tajemnic, nie zawsze uzasadnionych celem regulacji. Powodować to może trudności w ustaleniu zakresu i zasad stosowania określonych przepisów. Celowe wydaje się ujednolicenie terminologii i uproszczenie systemu ochrony tajemnic poprzez wprowadzenie wspólnych przepisów, które regulowałyby jednolicie określone grupy tajemnic. Racjonalność we wprowadzaniu tajemnic mogłoby wymusić ustalenie zasad konstruowania przepisów wprowadzających tajemnicę (minimalnych elementów), a zwłaszcza zobligowanie do wskazywania wartości, dla których są one ustanawiane, a które zwykle wymagają dekodowania nie tylko na podstawie ustaw regulujących tajemnice, ale również w oparciu o kodeksy deontologiczne. Dla zagwarantowania możliwie szerokiego dostępu do informacji publicznej, przy jednoczesnej elastyczności i uwzględnianiu konieczności ochrony określonych wartości, korzystne byłoby wprowadzenie katalogu wartości chronionych w ustawie o dostępie do informacji publicznej, a także testów szkody i ważenia interesów, co pozwoliłoby organowi stosującemu prawo na decydowanie o udostępnieniu informacji chronionej, jeżeli interes publiczny w ujawnieniu informacji przeważałby nad chronionymi interesami. Ponadto dla zapewnienia pełniejszej ochrony zidentyfikowanych tajemnic

rozważania wymaga określenie wspólnych zasad ochrony tajemnic obejmujących m.in. oznaczanie dokumentów zawierających tajemnice, przetwarzanie informacji chronionych w systemach teleinformatycznych (w tym warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne wykorzystywane do przetwarzania tajemnic), określenie wymagań w zakresie bezpieczeństwa przetwarzania tajemnic czy dokumentacji opisującej sposób przetwarzania tajemnic oraz środków technicznych i organizacyjnych zapewniających ochronę tajemnic odpowiednią do zidentyfikowanych zagrożeń (szerzej w: Struktura regulacji tajemnic ustawowo chronionych, s. 273-327).

Mając na uwadze przyjęte kryteria wyróżnienia tajemnicy prawnie chronionej, wskazałam inne niż tajemnice ograniczenia jawności, które mogą mieć charakter prawny i pozaprawny (faktyczny). Wśród nich umiejscowić można wynikające z przepisów proceduralnych ograniczenia w dostępie do akt postępowań, szczególne warunki podmiotowe lub przedmiotowe udostępnienia informacji (np. konieczność wykazania interesu prawnego lub faktycznego), ograniczenia wynikające z trudności technicznych czy organizacyjnych. Ograniczenia jawności mogą być również skutkiem przyjętego sposobu udostępnienia informacji czy też z zakresu anonimizacji. Istotny wpływ na urzeczywistnienie zasady jawności wywiera również regulacja techniki prowadzenia danego zbioru (szerzej m.in. w: Podstawy prawne ograniczeń jawności w Polsce, s. 46-49).

Przeprowadzone badania doprowadziły do potwierdzenia hipotezy, że jawność rejestrów publicznych doznawać może ograniczeń formalnych (związanych z reglamentowaniem dostępu do określonych danych) i faktycznych związanych z techniką prowadzenia rejestru. Ograniczenia mogą dotyczyć zarówno danych podlegających wpisowi, dostępu do akt rejestrowych, jak i możliwości żądania odpisów czy innych dokumentów obrazujących stan rejestru. Ograniczenia konstruowane są w przepisach ustawowych w różny sposób w zależności od rejestru, celu dla którego został ustanowiony, charakteru lub zakresu podlegających wpisowi danych. Zazwyczaj zawęża się krąg podmiotów uprawnionych do dostępu do rejestru poprzez przyjęcie, że dostęp mają tylko określone podmioty lub określone podmioty i osoby, które wykażą interes prawny uzasadniający wgląd do rejestru. Ograniczenia dostępu mogą mieć również charakter przedmiotowy i dotyczyć tylko pewnych kategorii danych. Wyłączenie części informacji z udostępniania może być motywowane ochroną informacji niejawnych (rejestr patentowy), innych tajemnic ustawowo chronionych (rejestr dawców komórek rozrodczych i zarodków), jak również podyktowane ochroną prywatności podmiotów podlegających wpisowi (np. dostęp do danych podmiotowych z ewidencji gruntów i budynków). Jeśli przepis prawny wskazuje jakie podmioty i na jakich

zasadach mają dostęp do określonych danych rejestrowych, oznacza to istnienie ograniczonej jawności formalnej rejestru. Kontrowersje budzić może sytuacja, w której w przepisach odnoszących się do rejestru publicznego nie określono komu i na jakich zasadach prawo dostępu do treści rejestru przysługuje. W braku wyraźnej podstawy do dostępu proponować można oparcie dostępu na przepisach ogólnych – dotyczących praw strony w postępowaniu administracyjnym (dla rejestrów administracyjnych) lub cywilnym (dla rejestrów sądowych), wykorzystanie art. 217 KPA przewidującego wydawanie urzędowych zaświadczeń lub też ustawy o dostępie do informacji publicznej. Wskazuje się również, że w przypadku, gdy przepisy ustawy regulującej prowadzenie rejestru milczą, uznać należy, że prawo nieograniczonego dostępu do danych rejestrowych przysługuje każdemu (domniemanie jawności danych rejestrowych). Wydaje się jednak, że jest to koncepcja zbyt daleko idąca. Szeroka definicja rejestru publicznego w ustawie o informatyzacji, niezawierająca odniesienia do kryterium jawności skłania raczej do przyjęcia, że ustawodawca dopuszcza istnienie takich rejestrów publicznych, które stanowią zasób wewnętrzny administracji i które zasadniczo nie cechują się jawnością formalną. Przepisy ogólne regulujące dostęp do rejestrów publicznych podmiotów publicznych albo podmiotów niebędących podmiotami publicznymi, a realizujących zadania publiczne zawiera ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne (szerzej m.in. w: Podstawy prawne ograniczeń jawności w Polsce, s. 28-32, Jawność formalna ksiąg wieczystych w Polsce, s.264-310, Jawność formalna rejestru zastawów, s. 341-350, Jawność formalna ewidencji partii politycznych, s. 377-382, Komentarz do art. 24 [w:] G. Szpor, M. Durzyńska, A. Gryszczyńska, I. Kamińska, K. Mączewski, W. Radzio, Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne. Komentarz, Warszawa 2013, s. 224-226, Legal limitations of public access to spatial data in Poland, s. 50-67).

Przyjęcie, że dane rejestrowe stanowią informację publiczną i brak jest regulacji szczególnej dostępu do danych w ustawie zasobowej sprawia, że należy rozważyć czy dostęp do nich byłby możliwy w trybie ustawy o dostępie do informacji publicznej, z uwzględnieniem ograniczeń w niej przewidzianych. Jednak należy podkreślić odmiennność celów realizowanych przez regulacje odnoszące się do jawności formalnej rejestrów (które mogą być różne dla poszczególnych rejestrów i obejmują m.in. zapewnienie bezpieczeństwa obrotu czy ochronę osób działających w zaufaniu do treści rejestru), od celów regulacji dostępu do informacji publicznej (zapewnienie jawności działania organów państwa) i celów ponownego wykorzystywania informacji sektora publicznego (wykorzystanie komercyjnej wartości informacji sektora publicznego i zbudowanie na ich podstawie innowacyjnych produktów

i usług o wartości dodanej) (szerzej m.in. w: Komentarz do art. 24 [w:] G. Szpor, M. Durzyńska, A. Gryszczyńska, I. Kamińska, K. Mączewski, W. Radzio, Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne. Komentarz, Warszawa 2013, s. 237-249, Legal limitations of public access to spatial data in Poland, s. 50-67).

Informatyzacji zasobów towarzyszą również modyfikacje właściwości i kompetencji organów tradycyjnie prowadzących dany rejestr. Dochodzi również do rozdzielania obowiązków związanych z dokonywaniem wpisów, udzielaniem informacji – w tym zezwalaniem na wielokryterialne wyszukiwanie w zbiorze, utrzymaniem i zapewnieniem bezpieczeństwa baz danych rejestru. Nowe możliwości wykorzystania zinformatyizowanych baz skłaniają prawodawcę do rozszerzania celu prowadzenia rejestru, kręgu podmiotów, którym przyznano dostęp, czy wprowadzania nowych usług opartych o dane rejestrowe (szerzej m.in. w: Jawność formalna ksiąg wieczystych w Polsce, s. 265-289, Jawność formalna rejestru zastawów, s. 341-345).

Towarzyszące informatyzacji zmiany nie zawsze znajdują aksjologiczne uzasadnienie i często nie są poprzedzone rzetelną oceną skutków regulacji. Działania takie mogą powodować w konsekwencji zmniejszenie zaufania do państwa i traktowanie rejestrów publicznych jako kolejnego narzędzia inwigilacji. Dlatego część z nich poddawana została prze mnie analizie krytycznej. Brak szerszej refleksji nad optymalnym zakresem jawności formalnej rejestrów, czy kolizji jawności formalnej z prawami osób podlegających wpisowi, powoduje utożsamianie tradycyjnie rozumianej „jawności formalnej rejestru”, oznaczającej udostępnianie określonych danych z rejestru wszystkim lub uprawnionym podmiotom, z „otwartością”, „otwartym dostępem” czy „przeszukiwalnością”. Ze względu na zakres podlegających wpisowi danych oraz współczesne możliwości techniczne – w tym zwłaszcza możliwość łączenia zbiorów pochodzących z różnych źródeł – nieodzowne staje się poszukiwanie kompromisu pomiędzy jawnością rejestru a ochroną praw podmiotów w nim ujawnionych (szerzej m.in. w: Jawność formalna ksiąg wieczystych w Polsce, s. 265-289, 299-310, Legal limitations of public access to spatial data in Poland, s. 50-67, Cybersecurity of public registers in Poland: selected legal issues, s. 105-113, Postulaty zmian w zakresie jawności i bezpieczeństwa rejestrów publicznych, s. 183-197).

Na podstawie przeprowadzonych badań poświęconych regulacji jawności rejestrów publicznych sformułowałam postulaty zmian o charakterze ogólnym.

Po pierwsze, celowe jest ujednolicenie zakresu danych podmiotowych podlegających wpisowi i udostępnieniu lub ochronie, albowiem negatywną konsekwencją rozproszenia

regulacji oraz powstania znacznej liczby rejestrów charakteryzujących się różnym zakresem danych podlegających wpisowi i udostępnieniu są niespójności logiczne w systemie prawa. Wyważenie dóbr i wartości chronionych poprzez poszczególne rejestry, z ochroną prywatności oraz bezpieczeństwem publicznym skłania do ograniczenia zakresu danych (w tym zwłaszcza danych osobowych) udostępnianych z rejestrów publicznych online dla niezindywidualizowanych odbiorców (szerzej m.in. w: Jawność formalna ksiąg wieczystych w Polsce, s. 307-310, komentarz do art. 24 [w:] G. Szpor, M. Durzyńska, A. Gryszczyńska, I. Kamińska, K. Mączewski, W. Radzio, Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne. Komentarz, Warszawa 2013, s. 224-249).

Po drugie, w zależności od rejestru i celu jego prowadzenia postulować można wprowadzenie rozliczalności (tj. mechanizmów umożliwiających ustalenie, kto i jakie dane przeglądał lub pobierał), stopniowości dostępu (oznaczającej zdefiniowane zakresów danych dostępnych dla każdego online oraz zakresu danych, do których dostęp przysługiwał będzie jedynie określonym podmiotom) lub innych ograniczeń – w tym w szczególności zawężenia kręgu podmiotów uprawnionych do wglądu i pobierania odpisów, barier o charakterze organizacyjnym (zwłaszcza mechanizmów zakładających identyfikację, uwierzytelnienie lub autoryzację), czy też barier o charakterze finansowym (konieczność wniesienia opłat za odpisy, wyciągi, zaświadczenia lub wgląd do rejestru). Dla realizacji zasady rozliczalności celowe jest przyznawanie dostępu online do danych rejestrowych tylko dla osób o potwierdzonej tożsamości. Jako mechanizmy uwierzytelnienia można wykorzystać profil zaufany platformy ePUAP, podpisy elektroniczne, czy inne mechanizmy uwierzytelnienia oparte o tzw. zaufaną trzecią stronę (np. poprzez posiadane konto bankowe). W ten sposób nie zostanie ograniczony zakres dostępnych online danych, a jedynie będzie wprowadzona bariera techniczna – w postaci konieczności uwierzytelnienia. Dalej idącym ograniczeniem może być zawężenie dostępu online do informowania o treści wpisów i złożonych dokumentów poprzez odpisy, zaświadczenia i inne dokumenty wydawane za pośrednictwem środków komunikacji elektronicznej, czy też wprowadzenie stopniowalnego dostępu online do treści rejestru i określenia, jakie dane dostępne powinny być dla każdego online, jakie zaś tylko dla określonych podmiotów. W modelu tym konieczne jest wprowadzenie mechanizmów autoryzacji, tj. potwierdzenia, czy dany podmiot jest uprawniony do uzyskania dostępu do żądanego zasobu. Koncepcja ta wymaga określenia, jakie informacje byłyby widoczne dla każdego online, jakie podmioty miałyby dostęp do pełnej treści rejestru i jak weryfikować ich uprawnienia. Przy ograniczonym dostępie online, dla każdego widoczne powinny być jedynie

wybrane informacje z rejestru, które pozwalałyby na dokonanie wstępnego sprawdzenia stanu prawnego podlegającego ujawnieniu. Wśród udostępnianych online danych należy unikać umieszczania numerów PESEL (szerzej m.in. w: Jawność formalna ksiąg wieczystych w Polsce, s. 299-305, Cybersecurity of public registers in Poland: selected legal issues, s. 105-110).

Po trzecie, badania wskazują również celowość wprowadzenia dla podmiotów prowadzących rejestry publiczne ustawowego obowiązku dokonywania przed przystąpieniem do informatyzacji rejestru oceny wpływu informatyzacji na ochronę interesu publicznego oraz indywidualnego (w tym prywatności osób fizycznych), a także na bezpieczeństwo przetwarzanych danych. Ponadto podmioty prowadzące rejestry publiczne w systemach teleinformatycznych, przed podjęciem decyzji dotyczącej udostępnienia danych rejestrowych w trybie teletransmisji, powinny zostać zobligowane do oceny wpływu udostępnienia danych rejestrowych w systemach teleinformatycznych na ochronę interesu publicznego i indywidualnego (w tym prywatności osób fizycznych). Przed udostępnieniem danych z rejestru publicznego w sieciach wydzielonych lub sieci publicznej podmioty prowadzące rejestry publiczne powinny zostać zobligowane do opracowania zasad kontroli dostępu i zarządzania uprawnieniami, w tym również sformułowania wzorcowego katalogu ról dostępowych, warunków dostępu z uwzględnieniem stopniowości uprawnień dostępowych, mechanizmów uwierzytelnienia, a także analizy zasadności wprowadzenia stopniowalnego dostępu do danych ze wskazaniem, jakie dane dostępne powinny być dla poszczególnych kategorii użytkowników (Pojęcie i jawność rejestrów publicznych - uwagi wprowadzające, s. 29-36, Cybersecurity of public registers in Poland: selected legal issues, s. 105-110).

Po czwarte, niezbędne jest określenie granic i zasad dopuszczalności ponownego wykorzystywania danych z rejestrów publicznych w ustawach zasobowych, regulujących prowadzenie poszczególnych rejestrów, po wcześniejszym przeprowadzeniu analizy wpływu ponownego wykorzystania na interes publiczny i prywatny, a także ryzyk związanych z ochroną danych osobowych. W tym celu postulować można choć częściowe oparcie ograniczeń prawa do informacji publicznej i prawa ponownego wykorzystywania informacji sektora publicznego na „teście szkody” (*harm test*) oraz „teście ważenia interesów” (*balancing of interests*). Reguły ogólne mogłyby w tym zakresie zostać wprowadzone do ustawy o informatyzacji, ustawy o dostępie do informacji publicznej lub do ustawy o ponownym wykorzystywaniu informacji sektora publicznego. Ponadto ograniczyć należy możliwość przekazywania do ponownego wykorzystywania danych rejestrowych zawierających dane

osobowe bez przeprowadzenia uprzedniej ich anonimizacji. W sytuacji udostępniania danych zanonimizowanych zbadać należy ryzyko ponownej identyfikacji. Przywrócone powinno również zostać brzmienie klauzuli kolizyjnej z art. 1 ust. 2 ustawy o dostępie do informacji publicznej sprzed nowelizacji z 8.11.2013 r. (Dz.U. z 2013 r. poz. 1474), poprzez usunięcie fragmentu: „pod warunkiem że nie ograniczają obowiązków przekazywania informacji publicznej do centralnego repozytorium informacji publicznej, o którym mowa w art. 9b ust. 1, zwanym dalej «centralnym repozytorium»”, a pozostawienie brzmienia: „przepisy ustawy nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi” i jednocześnie uchylenie ust. 3 w art. 1 ustawy o dostępie do informacji publicznej (Pojęcie i jawność rejestrów publicznych - uwagi wprowadzające, s. 29-36, Jawność formalna ksiąg wieczystych w Polsce, s. 305-307, komentarz do art. 24 [w:] G. Szpor, M. Durzyńska, A. Gryszczyńska, I. Kamińska, K. Mączewski, W. Radzio, Ustawa z 17 maja 1989 r. – Prawo geodezyjne i kartograficzne. Komentarz, Warszawa 2013, s. 224-249, Cybersecurity of public registers in Poland: selected legal issues, s. 105-110).

Po piąte, istotnym zidentyfikowanym problemem jest również przyznawanie dostępu do rejestrów publicznych określonym grupom podmiotów (w tym zwłaszcza w drodze teletransmisji danych) bez jednoczesnego wyposażenia organu odpowiedzialnego za prowadzenie rejestru w stosowne uprawnienia do kontroli spełniania przez te podmioty obowiązków wynikających z przepisów prawa i decyzji, którą przyznano dostęp oraz prawo do ograniczenia lub pozbawienia dostępu do danych w sytuacji naruszenia przez dany podmiot warunków dostępu. Dlatego też postuluję wzmocnienie instrumentów o charakterze administracyjnoprawnym i wyposażenie organów rejestrowych lub podmiotów odpowiedzialnych za zabezpieczenie danych rejestrowych w uprawnienia do kontroli wnioskujących o dostęp do danych oraz tych, którym dostęp ten został udzielony. Organy rejestrowe powinny być uprawnione w szczególności do badania urządzeń lub systemów teleinformatycznych przeznaczonych do komunikowania się pomiędzy uprawnionymi podmiotami a rejestrem, zabezpieczeń technicznych i organizacyjnych właściwych dla przetwarzania danych osobowych, a także sposobu przetwarzania i przeznaczenia pobranych danych. Zdyscyplinuje to podmioty, które uzyskały dostęp, ograniczy ryzyko naruszeń danych osobowych oraz innych incydentów, a także zapewni wyższy poziom bezpieczeństwa przetwarzanych danych (szerzej w: Postulaty zmian w zakresie jawności i bezpieczeństwa rejestrów publicznych, s. 299-300).

Po szóste, niezbędne jest położenie nacisku na kwestie cyberbezpieczeństwa rejestrów publicznych. Cyberbezpieczeństwo to w języku prawnym „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”. Incydenty naruszające cyberbezpieczeństwo powodują zakłócenia świadczenia podstawowych usług dla państwa i obywateli. W piśmiennictwie wskazuje się, że rosnąca liczba incydentów wynika z pomijania kwestii bezpieczeństwa i ochrony informacji w projektowaniu systemów teleinformatycznych służących do prowadzenia rejestrów. Uchwalenie ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz.1560), stanowiącej implementację dyrektywy 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, str. 1—30) oraz liczne międzynarodowe i krajowe inicjatywy związane z przeciwdziałaniem i obsługą incydentów, wytyczają nową płaszczyznę publicznoprawnych badań procesów informacyjnych, prowadząc do *konstatacji*, że w związku ze zmianą sposobu prowadzenia rejestrów zmienione powinno zostać również podejście do zabezpieczania danych. Przeprowadzone badania wskazują, że celowe jest sformułowanie i konkretyzacja zadań publicznych odnoszących się rejestrów publicznych oraz przypisanie ich realizacji określonym podmiotom. Ustalenie podmiotów odpowiedzialnych oraz obowiązków dotyczących przygotowania schematów modelu danych i ich implementacji w modelu danych w systemach teleinformatycznych, przygotowania, aktualizacji i rozwoju systemów teleinformatycznych, w których prowadzone są rejestry, zasad i zakresu udostępnianych danych, zabezpieczenia danych przed utratą, zmianą, nieuprawnionym dostępem, powinno pozytywnie wpłynąć na zabezpieczenia rejestrów publicznych przed cyberatakami. Dla zwiększenia cyberbezpieczeństwa zasobów postuluje się przede wszystkim zdefiniowanie zasobów informacyjnych z punktu widzenia ich klasyfikacji jako infrastruktury krytycznej państwa. Po określeniu zakresu podmiotowego, przedmiotowego, każdy zasób informacyjny powinien zostać zaliczony do jednej z kategorii jako: istotny, znaczący lub też uzupełniający. Następnie dla poszczególnych zasobów należy dokonać wyboru modelu utworzenia i prowadzenia zasobów informacyjnych państwa. Aktualne doniesienia medialne dotyczące postępowań prowadzonych w sprawie nieuprawnionego dostępu do danych pochodzących z ksiąg wieczystych, ewidencji gruntów i budynków czy nieuprawnionego wykorzystania i obrotu bazami danych marketingowych wskazują, że zagrożenia mają realny charakter i należy przeciwdziałać im zarówno z wykorzystaniem instrumentów administracyjnych, cywilnych jak i karnych. Sankcje powinny być przy tym skuteczne, proporcjonalne

i odstrasżające (szerzej m.in. w: *Jawność formalna ksiąg wieczystych w Polsce*, s. 307-310, *Cybersecurity of public registers in Poland: selected legal issues*, s. 105-110, *Nowe zagrożenia bezpieczeństwa rejestrów publicznych*, s. 293-309).

5. Omówienie pozostałych osiągnięć naukowo-badawczych

Moje zainteresowania naukowe obejmują jurydyzację zagadnień informacyjnych, obejmującą wpływ informatyzacji zasobów na realizację zadań publicznych i mieszczą się zasadniczo w zakresie prawa administracyjnego. Zagadnienia informacyjne i procesy informatyzacji podmiotów realizujących zadania publiczne mają jednak interdyscyplinarny charakter i cechują się problemami występującymi na stykach dyscyplin.

Wiodącą metodą moich badań jest metoda dogmatyczna. W pracy badawczej koncentruję się na analizie instytucji prawnych, które cechuje doniosłość teoretycznoprawna i praktyczna. W moim dorobku naukowym znajdują się opracowania interdyscyplinarne oraz prace, których wnioski bazują na badaniach empirycznych.

W moim dorobku naukowym można wyodrębnić kilka obszarów badawczych:

Pierwszy obszar obejmuje badania nad wpływem informatyzacji na publiczne zasoby informacyjne i ich jawność. Badania w tym obszarze rozpoczęłam jeszcze przed uzyskaniem stopnia doktora nauk prawnych, koncentrując się na prawnych i organizacyjnych problemach informatyzacji systemu informacji o nieruchomościach i przepływie geoinformacji. Po uzyskaniu stopnia doktora nauk prawnych kontynuowałam interdyscyplinarne badania nad wpływem informatyzacji na funkcje rejestru. Ich wyniki zawarłam w zawierającej zmodyfikowaną treść rozprawy doktorskiej książce **„Nowa Księga Wieczysta. Informatyzacja rejestru publicznego”**, LexisNexis, Warszawa 2011. W monografii tej poddałam analizie publicznoprawne aspekty modernizacji ksiąg wieczystych i wskazałam, że informatyzacja nie może być pojmowana jedynie jako zmiana techniki prowadzenia rejestru, ponieważ wpływa na uregulowanie działań normatywnie postulowanych dla realizacji celów rejestru oraz działania realnie obserwowane dla ich urzeczywistnienia. Tym samym zmiana przepisów oraz działań faktycznych, oddziałuje na funkcje rejestru oraz uprawnienia podmiotów korzystających z tej instytucji. Badania nad elektronicznym dostępem do Elektronicznej Księgi Wieczystej i KRS zawarłam w rozdziale **„Elektroniczny dostęp do Nowej Księgi Wieczystej i Krajowego Rejestru Sądowego”** opublikowanym w monografii *„Internet. Prawno-informatyczne problemy sieci, portali i e-usług”*, pod red.

G. Szpor i W.R. Wiewiórowski, C.H.Beck, Warszawa 2012, s. 289-303, zaś częściowe badania dotyczące formalnej jawności rejestrów sądowych w rozdziale **„Wpływ informatyzacji na formalną jawność rejestrów sądowych”**, opublikowanym w monografii „Ewolucja prawa polskiego pod wpływem technologii informatycznych. Elektroniczne aspekty wymiaru sprawiedliwości”, red. G. Tylec, J. Misztal – Konecka, Wydawnictwo KUL, Lublin 2012, s. 129-148. W publikacjach tych zaproponowałam w szczególności wyodrębnienie nowej kategorii pojęciowej obok jawności formalnej zwykłej i rozszerzonej, którą byłoby upublicznienie danych w Internecie. Nowa kategoria odzwierciedlałaby znaczące rozszerzenie zakresu jawności, powiązane z dostępnością danych online. Prawne problemy ponownego wykorzystywania informacji sektora publicznego podjęłam w artykule **Centralne repozytorium informacji publicznej** (Kwartalnik Prawa Publicznego nr 3/2012, s. 125-137), krytycznej ocenie poddając celowość wyodrębniania dodatkowego trybu udostępniania wybranych informacji publicznych. Porównałam również zakres gromadzonych danych oraz zasad udostępniania informacji w Biuletynie Informacji Publicznej (BIP) i centralnym repozytorium (CRIP).

W publikacji **„Finansowanie rejestrów sądowych”** zamieszczonej w monografii „Internet. Bazy danych i big data w sferze publicznej”, red. G.Szpor, C.H.Beck, Warszawa 2014, s. 191-208, dokonałam analizy wpływu funkcji fiskalnej na urzeczywistnienie innych funkcji. Pozwoliło to na wskazanie, że nadmiernie rozbudowana funkcja fiskalna może faktycznie wzmocnić funkcję selekcyjną i osłabić funkcję ewidencyjną, co jest zjawiskiem niepożądanym w przypadku rejestrów, w których dąży się do powszechności systemu i gdzie dla bezpieczeństwa obrotu prawnego wskazane jest takie ukształtowanie opłat, aby nie stanowiły one faktycznej bariery w ujawnieniu okoliczności podlegających wpisowi.

W projekcie Model Regulacji Jawności w oparciu o przygotowaną przeze mnie metodologię, pogłębionej analizie zostały poddane przepisy odnoszące się do jawności i jej ograniczeń z obszaru referencyjnego rejestrów publicznych. Wyniki badań prowadzonych przez zespół złożony z 18 autorów zostały opublikowane w liczącej około 35 arkuszy wydawniczych monografii zatytułowanej „Rejestry publiczne. Jawność i operacyjność”. Podsumowanie kluczowych ustaleń zawiera rozdział **„Postulaty dotyczące jawności rejestrów publicznych i jej ograniczeń”** autorstwa A. Gryszczyńskiej, P. Drobka, A. Piskorz-Ryń (s. 645-649). Wyniki badań z tego obszaru badawczego prezentowałam również na kilku międzynarodowych i kilkunastu krajowych konferencjach naukowych (m.in. na międzynarodowej konferencji "Funkcje ksiąg wieczystych w ujęciu prawnoporównawczym", która odbyła się 23 kwietnia 2014 r. w Akademii im. Jana Długosza

w Częstochowie, w ramach projektu Narodowego Centrum Nauki w Krakowie, na międzynarodowej konferencji „Jawność rejestrów publicznych a regulacja dostępu do danych z ksiąg wieczystych i katastru nieruchomości”, która odbyła się 22 maja 2014 r. na UKSW, w ramach projektu MRJ, na konferencji naukowej „Modelowanie dostępu do informacji”, która odbyła się w dniach 4 -14 sierpnia 2015 r.). Badania oraz kwerendę biblioteczną w tym obszarze badawczym prowadziłam oraz prezentowałam również podczas pobytu na uniwersytecie w Bari (L'Università degli Studi di Bari Aldo Moro) w 2013 roku w ramach programu LLP Erasmus, gdzie wygłosiłam wykład L'accesso ai registri elettronici pubblici in Polonia sull'esempio dei registri dell'immobilità e delle aziende (Dostęp do elektronicznych rejestrów publicznych w Polsce na przykładzie rejestrów nieruchomości oraz przedsiębiorców).

Drugi obszar badawczy obejmuje prawną regulację tajemnic. Od 2013 roku prowadziłam badania dotyczące tajemnic prawnie chronionych koordynując zadanie w projekcie MRJ. Ich celem było wykonanie kompleksowego przeglądu przepisów prawnych odnoszących się do realizacji zasady jawności i jej ograniczeń dla weryfikacji hipotezy o nadmiarowości regulacji ograniczeń jawności oraz niespójności przepisów w tym zakresie. W realizacji celów zadania udział wzięło 44 wykonawców, którzy przygotowali opracowania o łącznej objętości około 80 arkuszy wydawczych, które zostały następnie opublikowane w tomie VI monografii „Jawność i jej ograniczenia. **Struktura tajemnic**” (wydanie I – 2014 r., wydanie II rozszerzone -2016 r.) oraz w cyklu „**Leksykon tajemnic**” opublikowanym w 50 kolejnych numerach Monitora Prawniczego (począwszy od numeru 23/2013 MoP). W ramach przeprowadzonych badań, analizie poddano: podstawy prawne tajemnic, sposób wprowadzenia ochrony określonych informacji, wartości podlegające ochronie, zakres przedmiotowy i podmiotowy tajemnic, okres ochronny, podmioty uprawnione, kryteria i zasady dostępu do informacji objętych tajemnicą, regulację zasad przetwarzania informacji objętych tajemnicą, sankcje za nieuprawnione ujawnienie informacji oraz relacje z innymi tajemnicami. Wśród szczegółowych opracowań naukowych poświęconych poszczególnym tajemnicom znajdują się również opracowania mojego autorstwa: **Tajemnica rzeczoznawcy majątkowego**, Monitor Prawniczy 2015/22, s. 1229-1232, **Tajemnica detektywa i przedsiębiorcy wykonującego działalność gospodarczą w zakresie usług detektywistycznych**, Monitor Prawniczy 2015/23, s. 1277-1281, **Tajemnica korespondencji**, Monitor Prawniczy 2015/24, s. 1335-1342, **Tajemnica prokuratorska**, Monitor Prawniczy 2014/10, s. 545-552. Jestem również współautorką zaktualizowanego przeglądu podstaw

prawnych obowiązku zachowania tajemnicy (A. Gryszczyńska, K. Mordaszewski, P. Potejko, C. Rybak, **Klasyfikacja podstaw prawnych obowiązku zachowania tajemnicy**, w: *Jawność i jej ograniczenia*, red. G. Szpor, Tom VI Struktura tajemnic, red. A. Gryszczyńska, C.H.Beck, Warszawa 2016 (wydanie II), s. 329-455) oraz współredaktorką **Leksykonu tajemnic** (G. Szpor (red.), A. Gryszczyńska (red.), *Leksykon tajemnic*, C.H.Beck, Warszawa 2016), który prezentuje wyniki badania regulacji prawnej tajemnic i zawiera 162 hasła, w których zebrano wskazywane przez przedstawicieli piśmiennictwa i judykaturę tajemnice prawnie chronione. Jestem również autorką 11 haseł, a także współautorką 46 haseł i Wstępu.

Złożoną problematykę podstaw prawnych ograniczeń dostępu do danych przestrzennych w prawie międzynarodowym i europejskim oraz prawie wybranych krajów zawarłam w rozdziale „**Prawne aspekty jawności danych przestrzennych i ich ograniczeń**” (G. Szpor (red.), A. Gryszczyńska (red.), *Access to spatial data and its limitations. Legal aspects*, Zagreb 2015 r., ISBN 978-953-6129-52-2). Badaniem objęto akty prawne wprowadzające ograniczenia dostępu do określonych informacji o charakterze podstawowym i ogólnym oraz wybrane przepisy o charakterze szczególnym. Badano również czy implementacja dyrektywy INSPIRE przyczyniła się do uporządkowania przepisów regulujących dostęp do danych przestrzennych i formułujących ograniczenia czy szczególne warunki ich udostępnienia.

Wyniki badań z tego obszaru badawczego prezentowałam na kilkunastu krajowych konferencjach naukowych (m.in. konferencji naukowej pod patronatem Marszałka Sejmu - "Perspektywy zmian regulacji jawności i jej ograniczeń", która odbyła się 20.10.2014 r. w Sejmie RP, II Kongresie Elektryki Polskiej, który odbył się w dniach 1-2.12.2014 r. w Warszawie, VII Konferencji naukowej „Bezpieczeństwo w Internecie: Internet Rzeczy. Bezpieczeństwo Smart City”, która odbyła się w dniach 14 -15 maja 2015 r. w UKSW) oraz na szkoleniach praktycznych dla funkcjonariuszy publicznych.

Trzeci obszar badawczy obejmuje prawne aspekty cyberbezpieczeństwa i przeciwdziałania cyberprzestępczości. Jest to obszar na którym szczególnie skupiam zainteresowania badawcze od 2016 roku i gdzie łączę badania naukowe z doświadczeniami praktycznymi związanymi z prowadzeniem jako prokurator najbardziej skomplikowanych postępowań z zakresu cyberprzestępczości. Za interdyscyplinarność, łączenie aktywności naukowej i praktyki prawniczej, w tym nowym i skomplikowanym pod względem prawnym oraz praktycznym obszarze, zostałam nagrodzona w 2016 r. w konkursie *Rising Stars Prawnicy* – liderzy jutra.

Badania w zakresie cyberbezpieczeństwa z uwagi na zainteresowania rejestrami publicznymi pierwotnie koncentrowały się wokół bezpieczeństwa rejestrów i danych rejestrowych i częściowo został ujęte w monografii „Rejestry publiczne. Jawność i interoperacyjność”. W 2017 roku pod moją współredakcją została wydana monografia **„Internet. Strategie bezpieczeństwa”** (red. G. Szpor, A. Gryszczyńska; C.H. Beck, Warszawa 2017), w której analizowano nowe zagrożenia związane z cyberprzestępczością i cyberterroryzmem a także działania mające na celu zapewnienie bezpieczeństwa w cyberprzestrzeni, do których zaliczono zwłaszcza działania legislacyjne i normalizacyjne, zdefiniowanie zadań publicznych związanych z zapewnieniem ładu w cyberprzestrzeni, a także określenie podmiotów odpowiedzialnych za cyberbezpieczeństwo i ich kompetencji.

W 2017 roku brałam udział w pracach nad opinią dotyczącą projektu ustawy o krajowym systemie cyberbezpieczeństwa. Jestem również współredaktorką i współautorką pierwszego i dotychczas jedynego komentarza do ustawy o krajowym systemie cyberbezpieczeństwa (G. Szpor (red.), A. Gryszczyńska (red.), K. Czaplicki (red.), **Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz** (autorstwo w zakresie Wprowadzenia - p.I i komentarzy do rozdziałów **„Obowiązki dostawców usług cyfrowych”** (art. 17–20) oraz **„Zadania ministra właściwego do spraw informatyzacji”** (art. 45–50), Wolters Kluwer Warszawa 2019).

Pojawianie się nowych zagrożeń związanych z tworzeniem i dystrybucją oprogramowania ransomware oraz przeprowadzenie największego według Europolu ogólnosiwiatowego ataku z wykorzystaniem złośliwego oprogramowania WannaCry w maju 2017 roku skłoniły mnie nie tylko do analizy technicznej incydentów z wykorzystaniem oprogramowania szyfrującego, ale również do określenia prawnokarnych podstaw ich penalizacji oraz wskazania niezbędnych do wykonania w toku postępowania czynności, które mogą doprowadzić do wykrycia sprawców. Ponieważ dla skutecznego zwalczania cyberprzestępczości niezbędne jest podjęcie działań wielopłaszczyznowych oraz międzyinstytucjonalna współpraca pomiędzy organami ścigania i wymiaru sprawiedliwości, zespołami CERT/CSIRT, czy prywatnymi podmiotami zajmującymi się cyberbezpieczeństwem, przedmiotem analiz uczyniłam również prawne aspekty współdziałania podmiotów tworzących krajowy system cyberbezpieczeństwa i przedstawiłam wnioski płynące z ćwiczeń CyberPOL Exercises 2017 #1, w których brałam udział. Ustalenia z tego zakresu zawarłam w rozdziale **„Prowadzenie postępowań karnych w sprawach z zakresu dystrybucji ransomware”** monografii [w:] *Przestępczość Teleinformatyczna 2018*, red. J. Kosiński, Gdynia 2019 , s.193-218, ISSN 1898-3189 (w druku).

Wyniki badań w zakresie prawnych aspektów cyberbezpieczeństwa i przeciwdziałania cyberprzestępczości prezentowałam na kilku międzynarodowych i kilkudziesięciu krajowych konferencjach naukowych, wielokrotnie podczas wystąpień konferencyjnych formułując postulaty zmian ustawy o świadczeniu usług drogą elektroniczną, a także regulacji odnoszących się do ukształtowania odpowiedzialności karnej za kradzież tożsamości i przestępstwa przeciwko ochronie informacji. Wskazywałam również na niedostatki w ukształtowaniu zasad współpracy i wymiany danych pomiędzy podmiotami zajmującymi się obsługą incydentów (m.in. podczas międzynarodowej konferencji 21st Annual IBA Transnational Crime Conference (16 – 18.5.2018 r., Kraków), międzynarodowej konferencji Authentication and admissibility of electronic evidence” (8-9.6.2017 r., Londyn), XXII Międzynarodowej Konferencji SECURE 2018 (23-24.10.2018 r., Warszawa), XX Międzynarodowej Konferencji Techniczne Aspekty Przestępczości Teleinformatycznej (12-14.6.2017 r., Szczytno), Międzynarodowej Konferencji Naukowo-Praktycznej "Internetowe naruszenia własności intelektualnej" (28-29.9. 2016 r., Szczytno), XXI Konferencji Naukowej Techniczne Aspekty Przestępczości Teleinformatycznej (29-30.5.2018, Szczytno), IV Konferencji Naukowej Przestępczość Teleinformatyczna (9-11.9.2018 r., Gdynia), Security Case Study 2018 (13-14.9.2018 r., Warszawa), Tel Sec (17 -18.10.2018 r., Serock), Advanced Threat Summit 2018 (13-14.11.2018 r., Warszawa), What the h@ck (1.12.2018 r., Warszawa), XII Forum Bezpieczeństwa I Audytu IT Semafor 2019. Wojny Informacyjne (14-15.3.2019 r., PGE Narodowy w Warszawie). W tym zakresie brałam również udział w międzynarodowych szkoleniach organizowanych przez Academy of European Law i European Judicial Training Network oraz prowadziłam szkolenia dla prokuratorów, sędziów, przedstawicieli innych zawodów prawnych, funkcjonariuszy policji, CBA. Jestem również autorką metodyki z zakresu zwalczania cyberprzestępczości przygotowanej dla sędziów oraz rozbudowanego szkolenia e-learningowego z tego zakresu dla prokuratorów.

Czwartym obszarem badawczym są prawne aspekty ochrony informacji, w tym w szczególności danych osobowych. Na tym polu analizowałam odpowiedzialność karną za naruszenie prawa do informacji publicznej, odpowiedzialność karną za naruszenie obowiązku zachowania tajemnicy oraz odpowiedzialność karną za naruszenie ochrony danych osobowych. Jestem autorką rozdziałów w monografiach naukowych **„Odpowiedzialność karna za naruszenie prawa do informacji publicznej a prawnokarne konsekwencje naruszenia obowiązku zachowania tajemnicy”**, w: Jawność i jej ograniczenia, red. G. Szpor, Tom IV Znaczenie orzecznictwa, red. M. Jaśkowska, C.H. Beck, Warszawa 2014, s. 305-322

oraz „**Karnoprawna ochrona danych przestrzennych wobec nowych zagrożeń związanych z rozwojem cyberprzestępczości**”, w: Internet. Informacja przestrzenna, red. Grażyna Szpor, K. Czaplicki, C.H. Beck; Warszawa 2018, 151-171, ISBN 978-83-815-8157-8. W pracach wskazywałam, że zarówno zasady dostępu do informacji publicznej, jak i regulację prawną odnoszącą się do tajemnic ustawowo chronionych cechuje brak przejrzystości, co powoduje poważne implikacje dla reakcji prawnokarnej. Osoby zobowiązane do udostępnienia informacji publicznej często stawiane są przed dylematem związanym z decyzją co do udostępnienia informacji publicznej z uwagi na świadomość karnoprawnych sankcji za jednocześnie udostępnienie informacji stanowiących tajemnicę czy też udostępnienie podlegających ochronie danych osobowych. Stąd przepis art. 23 ustawy o dostępie do informacji publicznej, choć nie jest „martwy”, jak wskazują niektórzy przedstawiciele piśmiennictwa, jest mało efektywny, a wobec problemów z interpretacją podstawowych pojęć z ustawy o dostępie do informacji publicznej, przekładających się następnie na występowanie błędów co do znamion czynu zabronionego, jego praktyczne znaczenie jest znikome.

Wyraziłam również pogląd, że w świetle narastających zagrożeń związanych z rozwojem cyberprzestępczości celowa jest dyskusja nad wysokością sankcji karnych – zwłaszcza za uzyskiwanie nieuprawnionego dostępu do informacji w wyniku przełamania lub ominięcia zabezpieczeń. W tym zakresie zaproponowałam wprowadzenie w art. 267 KK typu kwalifikowanego przewidującego surowszą odpowiedzialność karną za uzyskanie bez uprawnienia dostępu do danych osobowych poprzez ominięcie lub przełamanie zabezpieczeń a także inne ukształtowanie odpowiedzialności karnej za kradzież tożsamości.

Analiza zakresu podmiotowego i przedmiotowego ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości skłoniła mnie do wyrażenia krytycznej opinii w zakresie poprawności implementacji Dyrektywy 2016/680 (Dz. Urz. UE L Nr 119, s. 89 ze zm). Ograniczenia zakresu podmiotowego i przedmiotowego mocno zawężają zakres stosowania ustawy, zaś wyłączenia oraz liczne przepisy wprowadzające modyfikacje zasad i warunków ochrony danych osobowych, a także praw osób, których dane są przetwarzane w ustawach szczególnych, prowadzą do znacznego rozproszenia i braku jednolitości regulacji. Przy ustaleniu, że w zakresie wyłączeń podmiotowych i przedmiotowych wskazanych w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości transpozycja dyrektywy 2016/680 nie nastąpiła, należy rozważyć, czy podstawą ochrony takich danych osobowych nie będą w dalszym ciągu przepisy ustawy z 29.8.1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.), ponieważ nie został zrealizowany warunek

wskazany w art. 175 ustawy o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm), przywołany również w art. 107 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz.U. z 2019 r. poz. 125 (**Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – zakres przedmiotowy i podmiotowy** [w:] Internet. Przetwarzanie danych, red. G. Szpor, K. Czaplicki, C.H. Beck, Warszawa 2019).

Analizie poddawałam również zasady przenoszenia danych osobowych wskazując wątpliwości związane w szczególności z ustaleniem zakresu przenoszonych danych (w tym m.in. metadanych, cookies, danych o charakterze technicznym, statystycznym czy treści przetwarzanej w danym serwisie przez użytkownika), formatów w jakich mają być one przenoszone, ochrony praw własności intelektualnej i tajemnicy przedsiębiorstwa czy bezpieczeństwem danych przy wykonywaniu prawa do ich przeniesienia (**Prawo do przenoszenia danych osobowych** [w:] Realizacja praw osób których dane są przetwarzane, red. B. Fischer, M. Sakowska – Baryła, Wrocław 2017, s. 263-288).

Jestem również autorką opracowań popularnonaukowych publikowanych w kwartalniku ABI Expert (Czy potrzebna jest karnoprawna ochrona danych osobowych?, ABI Expert 2/2018, Czy ochrona danych wymaga odpowiedzialności karnej?, ABI Expert 1/2018, s. 9, Zgoda na przetwarzanie danych osobowych w sektorze publicznym w świetle regulacji ogólnego rozporządzenia o ochronie danych, ABI Expert 2/2017). Wyniki badań prawnych aspektów ochrony informacji prezentowałam na licznych krajowych konferencjach naukowych (m.in. na X Konferencji Naukowej Bezpieczeństwo w Internecie. Przetwarzanie danych osobowych (25-26.5.2018, Warszawa), Forum Administratorów Bezpieczeństwa Informacji (3-4.4.2017 r.), konferencji Ochrona danych osobowych w kontekście zmian prawa (22.5.2017 r., Gdańsk).

Piąty obszar badawczy obejmuje prawne problemy elektronicznych usług publicznych. W tym zakresie koncentrowałam się tylko na wybranych prawnych problemach identyfikacji osób korzystających z elektronicznych usług publicznych. Analizie poddawałam poziom zaawansowania e-usług w Polsce (**Stan budowy elektronicznej administracji w Polsce na tle pozostałych krajów Unii Europejskiej**, w: Wizja europejskiego społeczeństwa informacyjnego i jej realizacja w prawie polskim, red. G. Tylec, J. Misztal – Konecka, Wydawnictwo KUL, Lublin 2012, s. 95-115). Kontynuowałam też badania dotyczące wykorzystania podpisów elektronicznych rozpoczęte w 2015 r. (**Weryfikacja tożsamości osób korzystających z elektronicznych usług publicznych** [w:] Internet. Ochrona wolności,

własności i bezpieczeństwa, red. G. Szpor, C.H.Beck, Warszawa 2011, s. 236-245 oraz A. Gryszczyńska, K. Czaplicki, **Methods of identity verification of users of electronic public services illustrated with an access to geoinformation** [w:] The Future with GIS, red. D. Kerekovic, GIS Forum, Zagreb 2011, s. 205-210.

Szczegółowy wykaz dorobku habilitacyjnego zawierający m.in. wykaz wygłoszonych referatów, udział w projektach badawczych oraz informację o osiągnięciach dydaktycznych, współpracy naukowej i popularyzacji nauki zawierają załączniki nr 4 i 5