Autoreferat

„Prawne gwarancje zrównoważonego przetwarzania informacji w czasach Big Data"

1. Imię i Nazwisko.

   Wojciech Rafał Wiewiórowski

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

   - **Doktor nauk prawnych (2000), Wydział Prawa i Administracji Uniwersytetu Gdańskiego; praca doktorska z prawa konstytucyjnego pt.: *„Sądowa interpretacja zasady podziału władzy i rola ustrojowa sądów w Stanach Zjednoczonych Ameryki"*;**

   - **Magister prawa, Wydział Prawa i Administracji Uniwersytetu Gdańskiego; praca magisterska z prawa morskiego pt.: *„Współpraca międzynarodowa w ramach Konwencji o ochronie środowiska morskiego obszaru Morza Bałtyckiego"*.**

   - **Dyplom ukończenia *"English and European Law School"* – programu prowadzonego przez British Law Centre Uniwersytetu w Cambridge oraz Wydział Prawa i Administracji Uniwersytetu Gdańskiego (1997);**

   - **Dyplom ukończenia studiów specjalnych z zakresu wiedzy dydaktycznej dla nauczycieli - Gdańska Wyższa Szkoła Administracji (2004);**

   - **Dyplom ukończenia *"Singapore Co-operation Programme. eGovernment - Journey Towards Public Sector Excellence"* w Civil Service College w Singapurze (2009).**

3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych/ artystycznych.

   - **Wydział Prawa i Administracji Uniwersytetu Gdańskiego - od 2003 r.**
     Adiunkt,
     Kierownik Pracowni Informatyki Prawniczej (w latach 2003-2010),

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 (Dz. U. z 2017 r. poz. 1789):

   a) tytuł osiągnięcia naukowego/artystycznego,

   Cykl powiązanych ze sobą tematycznie publikacji wydanych po uzyskaniu stopnia doktora nauk prawnych, z lat 2008-2019, zatytułowany „Prawne gwarancje zrównoważonego przetwarzania informacji w czasach Big Data". Na cykl składają się następujące pozycje (na liście zastosowano porządek chronologiczny, w dalszej części autoreferatu zastąpiony porządkiem merytorycznym):

   1. *Konosament a blockchain. Możliwości wykorzystania technologii rozproszonego rejestru dla celów „elektronicznego indosu" przy przenoszeniu praw z papierów wartościowych na zlecenie* [współautorka] I. Zużewicz-Wiewiórowska, [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek [red.:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane,* Warszawa 2019, s.125-153, ISBN 978-83-8158-596-5
   2. *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych,* „Europejski Przegląd Sądowy", Nr 5, 2017, s. 23-31;
   3. *Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy* [w:] G. Vermeulen, E. Lievens [red.:] *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data,* Maklu, Antwerp-Apeldoorn-Portland 2017, s. 171-192, ISBN 978-90-466-0910-1,
   4. *Inwigilacja w celu zapewnienia bezpieczeństwa publicznego. Cztery filary dopuszczalnej ingerencji w prawo do prywatności,* „Disputatio. Przegląd Naukowy", T. 24, 2017, s. 125-143;
   5. *Re-use of Maritime Passengers' PNR Data for Public Security Purposes*, [współautorka] I. Zużewicz-Wiewiórowska, „Prawo Morskie", T. 33, 2017, s. 137-154;

6. *Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach big data* [w:] *Jawność i jej ograniczenia, t. 12, Model regulacji* [red.:] T. Bąkowski, G. Szpor, C. H. Beck, Warszawa 2016, s. 1-69, ISBN: 978-83-255-8822-9, ISBN: 978-83-255-8823-6 (e-book);
7. *Dane osobowe w inteligentnym mieście korzystającym z rozwiązań Internetu rzeczy* [w:] *Internet rzeczy bezpieczeństwo w smart city* [red.:] G. Szpor, C.H.Beck, Warszawa 2015, ss. 315-334, ISBN: 978-83-255-7930-2;
8. *Ochrona prywatności jako ograniczenie prawa do ponownego przetwarzania informacji publicznej,* „Gdańskie Studia Prawnicze: Studia ustrojoznawcze: księga jubileuszowa profesora Andrzeja Pułło", T. 31, 2014, s. 145-155
9. *Proces przetwarzania danych z dokumentów elektronicznych w systemach teleinformatycznych e-Maritime* [współautorka] I. Zużewicz-Wiewiórowska, „Prawo Morskie", T. 30, 2014, s. 27-52;
10. *Kwanty informacji o osobie. Prawne aspekty przetwarzania danych o osobach i „obiektach" pochodzących z rozproszonych zbiorów* [w:] P., Z. Rau, M. Wągrowski [red.:] *Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa. Szanse i zagrożenia,* LEX Wolters Kluwer, Warszawa 2013, s. 1139-1147, ISBN 978-83-264-4255-1;
11. *Ponowne przetwarzanie informacji publicznej zawierającej dane osobowe* [w:] G. Sibiga [red.:] *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej,* C.H.Beck, Warszawa 2013, ISBN 978-83-255-6375-2, **s.** 392-400;
12. *Prawo do prywatności w systemie inteligentnych sieci*, „Monitor Prawniczy" - Dodatek 'Ochrona danych osobowych' [red.:] G. Sibiga, Nr 8 z 2013 r., s. 27-37;
13. *Profilowanie osób na podstawie ogólnodostępnych danych* [w:] A. Mednis [red.:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Wyd. WPiA Uniwersytetu Warszawskiego, Warszawa 2013, s. 25-40, ISBN 978-83-63093-94-5;
14. *Prawne aspekty udostępniania usług administracji publicznej w modelu chmury* [w:] G. Szpor [red.:] *Internet – Cloud computing. Przetwarzanie w chmurze*, C.H.Beck, Warszawa 2013, s. 83-120, ISBN 978-83-255-5235-0, e-book 978-83-255-5236-7;
15. *Legal Aspects of e-Governmental Clouds*, "International Journal on Information Technology and Security", Nr 1 z 2013 r., Sofia;

16. *Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa*, „Krajowa Rada Sądownictwa", Nr 1 z 2013 r., s. 13-26;
17. *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, „Monitor Prawniczy" - Dodatek 'Ochrona danych osobowych' [red.:] G. Sibiga, Nr 7 z 2012, s. 1-8;
18. *Privacy by Design jako paradygmat ochrony prywatności* [w:] G. Szpor, W. Wiewiórowski [red.:] *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*, C.H.Beck, Warszawa 2012, s. 13-29, ISBN 978-83-255-3908-5; e-book 978-83-255-3793-7;
19. *Prawna ochrona danych biometrycznych w systemach teleinformatycznych pracodawcy. Cele przetwarzania a zakres ochrony* [w:] A. Nerka, T. Wyka [red.:] *Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmian*, Wolters Kluwer Polska, Warszawa 2012, s. 17-26, ISBN 978-83-264-1685-9;
20. *Personal Profiling Based on Generally Accessible Data*, "International Journal on Information Technology and Security", Nr 3 z 2012 r., Sofia, s. 31-46;
21. *Privacy and the Liability of Intermediary Service Provider in the Clouds. E-Governmental Aspects* [w:] F. Zombor [red.:] *International Data Protection Conference 2011*, Magyar Kozlony Lap-Es Konyvkiado, Budapeszt 2011, s. 49-59, ISBN 978-963-9722-96-5;
22. *Automatyzacja rozstrzygnięć i innych czynności w sprawach indywidualnych załatwianych przez organ administracji publicznej* [współautor:] G. Sibiga [w:] J. Gołaczyński [red.:] *Informatyzacja postępowania sądowego i administracji publicznej*, C.H.Beck, Warszawa 2010, s. 229-242, ISBN 978-83-255-1396-2;
23. *Pojęcie referencyjności w dyskusji o zasobach informacyjnych państwa* [w:] M. Barczewski, K. Grajewski, J. Warylewski [red.:] *Prawne problemy wykorzystywania nowych technologii w administracji i wymiarze sprawiedliwości – III Konferencja Naukowa WPiA Uniwersytetu Gdańskiego oraz Wolters Kluwer Polska, Gdańsk, 20-21 października 2008 r.*, Wolters Kluwer Polska, Warszawa - Kraków 2009; s. 195-203, ISBN 978-83-264-0023-0;

b) **Omówienie celu naukowego prac i osiągniętych wyników**

Kolejne etapy informatyzacji procesów gospodarczych i administracyjnych i rosnąca rola środków komunikacji elektronicznej w życiu codziennym powodowały, że już od lat 70. XX w. wzrastało przekonanie, że istnieją podmioty, które uzyskują bądź mogą uzyskać dostęp do lawinowo rozwijających się zasobów informacyjnych i mogą wdrożyć sposoby przetwarzania informacji, które – nieznane nieświadomym uczestnikom rynku i obywatelom – mogą prowadzić do podejmowania wobec nich środków, których nie są świadomi i które wręcz mogą prowadzić do dyskryminacji osób, grup społecznych czy przedsiębiorców. Pierwotnie organizacją, która była w naturalny sposób oskarżana o chęć świadomego, acz ukrytego, przetwarzania rozproszonych danych w sposób, który może naruszać prawa i wolności, było państwo. Szybko rozprzestrzeniało się przekonanie, że praktyki potężnych rządów i korporacji w zakresie przetwarzania danych redukują jednostkę do statusu podmiotu danych, co zagraża prawom podstawowym i wolnościom. Już w latach 70. i 80. możemy przywołać liczne wezwania do ograniczenia takich praktyk lub wprowadzenia różnych mechanizmów kontroli nad działaniami państwa, a wkrótce również nad działaniami podmiotów rynkowych. W tym znaczeniu możemy powiedzieć, że zastrzeżenia wobec możliwości naruszania wolności i praw informacyjnych lub manipulowania wielkoskalowymi zasobami danych nie są niczym nowym. Tym jednak, co wyróżnia obecną falę zintegrowanego przetwarzania informacji przy wykorzystaniu technologii komunikacyjnych określanych terminem big data, jest wszechobecność takich działań i ich siła.

Prezentowany cykl publikacji opatrzony zbiorczym tytułem „Prawne gwarancje zrównoważonego przetwarzania informacji w czasach *Big Data*" został przygotowany celem wszechstronnego omówienia zagadnień prawnych i praktycznych pojawiających się w sytuacji, gdy rozbudowane zasoby informacyjne tworzone w procesie danetyzacji przestrzeni, w której żyje człowiek [Mayer-Schonberger, Cukier] stają się podstawą do tworzenia rejestrów publicznych w rozumieniu przyjętym w Polsce przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne [Szpor, Wojsyk]. Rejestry publiczne rozumiane jako zasoby informacyjne wykorzystywane przez jednostki publiczne [Stawecki] mogą stać się zasady rezerwuarami informacji publicznej możliwymi do wykorzystania w procesie dostępu do informacji publicznej oraz dowolnego przetworzenia – również dla celów gospodarczych – w ramach ponownego przetwarzania informacji sektora publicznego (PSI) [Bernaczyk, Piskorz-Ryń].

Takie działanie samo w sobie jest nie tylko dozwolone, ale wręcz zalecane przez prawo unijne, a informacja raz przekazana do użytku jako informacji sektora publicznego powinna być na podstawie przepisów PSI wykorzystywana w warunkach konkurencyjnych tak do celów publicznych jak i prywatnych. Tak komercyjnych, jak i niekomercyjnych [Sakowska-Baryła, Maciejewski].

Zrównoważenie przetwarzania takiej informacji powinno być dokonywane przy zastosowaniu narzędzi dostarczonych władzom publicznym i osobom których dane dotyczą przez zreformowane prawo ochrony danych osobowych w Unii Europejskiej. Ochrona danych osobowych wbudowana w całość procesu przetwarzania danych (*Privacy by Design* – PbD) powinna stać się paradygmatem przetwarzania informacji tak w sektorze publicznym jak i prywatnym. Stanowi więc cel polityki administracyjnej racjonalnego państwa rozumianej jako „uporządkowany zbiór wartości i zaniechań wyróżnionego w strukturze organizacyjnej systemu administracji publicznej podmiotu, ukierunkowanych na zmianę lub utrzymanie aktualnego stanu, a polegających na określeniu, zważeniu i wyborze istotnych dla podmiotu realizującego politykę administracyjną wartości" [Cieślak].

Wielokrotnie w ramach prezentowanego cyklu przypominam, że, dyskutując nad informacją publiczną, którą stanowi dana lub dane przechowywane w zasobach infrastruktury informacyjnej państwa, trzeba podkreślić, że wyjątkowo często pojawiającym się błędem jest zamienne stosowanie pojęć "danych" i "informacji". O ile w potocznym języku można utożsamiać posiadanie danych z posiadaniem informacji, o tyle w informatyce, na której opiera się całość dyskusji prawnej o zrównoważonej informacji w świecie *Big Data* pojęcia te – choć bliskoznaczne – nigdy nie stanowią synonimów. Dane są wartościami przechowywanymi w bazie rozumianymi wręcz jako wartości danego pola. Informacjami są zaś takie dane, które zostały przetworzone w sposób, uwidaczniający ich znaczenie i tym samym czyniący je użytecznymi.

Dane z rejestrów publicznych – stanowiących podstawowe zasoby infrastruktury informacyjnej państwa – w pobierane są w postaci dokumentu elektronicznego, czyli stanowiącego odrębną całość znaczeniową zbioru danych uporządkowanych w określonej strukturze wewnętrznej [Szpor, Wojsyk, Szostek]. Tak rozumiany dokument elektroniczny jest zupełnie innym pojęciem niż „dokument" bądź „dokument urzędowy" definiowany dla różnych gałęzi prawa. Przy rozważaniu dalszych kwestii należy pamiętać, że ze względu na to, że pozyskiwanie informacji do ponownego wykorzystania następować będzie z zasady w postaci

elektronicznej, przy tych regulowaniu tych czynności z zasady należy posługiwać się pojęciem „dokumentu elektronicznego".

Cykl jest wynikiem połączenia pracy naukowej na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego z pracą w administracji rządowej (2006-2010 - gabinet polityczny ministra odpowiedzialnego za dział informatyzacji, funkcja dyrektorem Departamentu Informatyzacji Ministerstwa Spraw Wewnętrznych i Administracji) oraz zajmowania stanowiska Generalnego Inspektora Ochrony Danych Osobowych – GIODO (2010-2014) oraz stanowiska Zastępcy Europejskiego Inspektora Ochrony Danych - EDPS /EIOD (od grudnia 2014 r.).

Przyjęte metody pracy naukowej mieściły się w klasycznym kanonie działań prawnika, będącego jednocześnie praktykiem administracji publicznej. Polegało to przede wszystkim na konceptualizacji i porządkowaniu zastanego materiału dogmatycznego, ocenie dotychczasowej doktryny i porównywaniu ich z kształtem rozwiązań rynkowych rozwijających się niekiedy w oderwaniu od aktualnego stanu prawnego (np. IoT, chmura, *blockchain*). Stosowałem klasyczne metody egzegezy tekstu prawnego od analizy systemowej przez metodę formalno-dogmatyczną i metodę historyczną po różne wersje wykładni funkcjonalnej i celowościowej. W mniejszym zakresie wykorzystano metody statystyczne. Niekiedy odwoływałem się do narzędzi naukowych nauk technicznych. Przyznać jednak należy, że wielokrotnie przy omawianiu zagadnień technicznych posługiwałem się samo samodzielnie tworzonymi rozwiązaniami jako, że powiązanie wprost polskiego języka prawnego i prawniczego z angielskojęzycznymi rozwiązaniami technicznymi, było prawie niemożliwe (np. prawne odpowiedniki elementów struktury bloku w *blockchainie*).

Struktura cyklu oparta była na zaproponowanej w publikacji określone jako oś cyklu systematyce, w naturalny sposób przechodząc od wstępnych rozważań o świecie *Big Data* i znaczeniu pojęć dane, informacja i dokument elektroniczny poprzez zagadnienia przetwarzania wielkich zasobów danych i związanych z tym zagrożeń po proponowane remedia, układając się w ciąg działów:

1. Przetwarzanie informacji w świecie big data
2. Informacja i jej zasoby
3. Wszechobecność danych. Danetyzacja przestrzeni prawnej
4. Wyniki operacji na dużych zasobach danych

5. Profile osobowe a zrównoważenie przetwarzania informacji

6. Rola Internetu rzeczy

7. Przetwarzanie w chmurze

8. Świt sztucznej inteligencji

9. Ochrona danych osobowych jako droga ku zrównoważeniu przetwarzania

1. Przetwarzanie informacji w świecie big data

Oś prezentowanego cyklu stanowi opublikowana w 2016 r. praca ***„Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach big data"*** (pozycja nr 6 na liście chronologicznej) stanowiąca główną część 12. tomu zbioru pt. *„Jawność i jej ograniczenia, t. 12, Model regulacji"* [red.: T. Bąkowski, G. Szpor], w której formułuję tezę, że informacja publiczna znajdująca się w zasobach informacyjnych infrastruktury informacyjnej państwa, będzie wykorzystywana – z użyciem PSI jako podstawy prawnej – do tworzenia profili osobowych, czyli do „automatycznej techniki przetwarzania danych polegającej na przypisaniu danej osobie 'profilu' w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji zachowań i postaw". Co więcej takie profile będą miały tak charakter tzw. „profili predykcyjnych" (tworzone w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie w szczególności poprzez uzupełnianie informacji publicznej o monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla, lub na które klika) jak i tzw. „profili jawnych" (tworzonych na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą).

Jednocześnie w związku z tym, że artykuł 1 Karty praw podstawowych Unii Europejskiej stanowi, że godność człowieka jest nienaruszalna i musi być szanowana oraz chroniona, nigdy wcześniej podstawowe prawa do prywatności i ochrony danych osobowych nie były tak istotne dla ochrony godności człowieka. Zapisane w traktatach stanowiących podstawę prawną konstrukcji Unii Europejskiej, w Karcie praw podstawowych Unii Europejskiej i w Konstytucji rzeczypospolitej Polskiej dają one człowiekowi możliwość rozwijania własnej osobowości, prowadzenia niezależnego życia, wykazywania się innowacyjnością oraz korzystania z innych praw i wolności. Zasady ochrony danych zdefiniowane zostały w Karcie praw podstawowych

UE i w ogólnym rozporządzeniu o ochronie danych – konieczność, proporcjonalność, rzetelność, minimalizacja danych, ograniczenie celu, zgoda i przejrzystość – mają zastosowanie do całego procesu przetwarzania danych, tak do gromadzenia, jak i do wykorzystywania. Technologia nie powinna narzucać wartości i praw, jednak relacji tej nie należy również sprowadzać do błędnej dychotomii. Z rewolucją cyfrową wiążą się obietnice korzyści w takich obszarach jak zdrowie, środowisko, międzynarodowy rozwój i efektywność ekonomiczna.

Zgodnie z planami Unii dotyczącymi stworzenia jednolitego rynku cyfrowego przetwarzanie w chmurze (*cloud computing*), Internet rzeczy (*Internet of Things* – IoT), duże zbiory danych oraz inne technologie uznaje się za klucz do konkurencyjności i wzrostu. Modele biznesowe wykorzystują nowe możliwości w zakresie masowego gromadzenia, natychmiastowego przesyłania, łączenia i ponownego wykorzystywania danych osobowych w celach, które są niemożliwe do przewidzenia i uzasadniane długotrwałymi i mało przejrzystymi politykami prywatności. Wszystko to sprawia, że zasady ochrony danych należy rozpatrywać w obliczu nowych wyzwań wymagających świeżego spojrzenia na sposób, w jaki są one stosowane. W dzisiejszym środowisku cyfrowym przestrzeganie prawa nie wystarcza – musimy wziąć pod uwagę wymiar etyczny przetwarzania danych. Ramy regulacyjne UE już teraz pozostawiają możliwość podejmowania elastycznych, zindywidualizowanych decyzji i określania takowych gwarancji, jeżeli chodzi o przetwarzanie danych osobowych. Dobrym krokiem naprzód będzie reforma ram regulacyjnych. Jednakże wpływ tendencji obserwowanych w opartym na danych społeczeństwie na godność, wolność jednostki i funkcjonowanie demokracji niesie ze sobą poważniejsze kwestie. Problemy te mają implikacje natury inżynierskiej, filozoficznej, prawnej i moralnej.

2. Informacja i jej zasoby

Od początku pracy nad tym projektem naukowym punktem początkowym dla wszystkich rozważań musi być teoria informacji [Stefanowicz, Hetmański, Wróblewski, Studnicki, Janowicz]. Już na potrzeby podręcznika „*Informatyka prawnicza. Technologia informacyjna dla prawników i administracji publicznej*" [współautor: G. Wierczyński], Kraków 2006, przygotowałem wstępne rozważania na temat roli informacji (rozwijane w kolejnych wydaniach podręcznika). Choć do cyklu nie włączam – z oczywistych względów – fragmentów wspomnianego podręcznika, to zwrócić należy uwagę, że opisane w nim zagadnienia

niedostrzeganych często przez legislatorów i przez doktrynę różnic pomiędzy pojęciami danych, informacji, dokumentu i dokumentu elektronicznego powraca wielokrotnie w kolejnych publikacjach włączonych do cyklu stanowiąc podstawę kolejnych kierunków rozważań nad zrównoważonym przetwarzaniem danych.

W znaczeniu przyjmowanym w teorii informacji dokumentem elektronicznym (rzadziej określanym jako dokument cyfrowy) jest utrwalona informacja (dokument) z sygnałem utrwalonym na nośniku elektronicznym, będąca komunikatem języka naturalnego w subkodach akustycznych lub graficznych [Bojar, Narojczyk]. Według definicji technicznej dokumentem elektronicznym jest dokument istniejący w postaci elektronicznej i dostępny za pośrednictwem techniki komputerowej (norma PN-ISO 690-2). Brak jest jednej wspólnej definicji dokumentu elektronicznego na potrzeby prawa nie tylko w wymiarze międzynarodowym, ale nawet krajowym. W większości systemów prawnych nie wykształcono jednolitego rozumienia terminu i z tego powodu bywa on definiowany kontekstowo, niekiedy na potrzeby pojedynczego aktu prawnego. W prawie polskim definicja gałęziowa została ustalona jedynie dla prawa administracyjnego. W ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne za dokument elektroniczny uznano stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. O ile definicja zawarta w ustawie o informatyzacji jest często traktowana jako systemowa dla całego polskiego prawa publicznego, o tyle w doktrynie i orzecznictwie nie ma wątpliwości, że nie można jej wprost zastosować dla prawa cywilnego i karnego [Szostek, Jacyszyn, Przetocki, Wittlin, Zakrzewski, Kocot, Górska, Janowski].

Zadanie prawidłowego skonstruowania szkieletu infrastruktury informacyjnej państwa [Oleński, Szafrański] należy rozpocząć od realizacji postulatu unikania zbędnej redundancji danych rejestrowych. W swoich pracach poddałem krytyce skonstruowaną w ostatnich latach w doktrynie prawa administracyjnego koncepcję tworzenia rejestrów referencyjnych (czasem nazywanych bazowymi). Rejestry takie miałyby spełniać w infrastrukturze informacyjnej szczególne funkcje, a standardy informacyjne stosowane w nich miałyby być normami obligatoryjnymi dla całego sektora publicznego. Rejestry referencyjne mają zdaniem twórców koncepcji przekazywać lub udostępniać – na zasadzie obowiązku ustawowego – dane do wszystkich systemów informacyjnych sektora publicznego, w zakresie wynikającym z funkcji tych systemów informacyjnych. Wszystkie pozostałe rejestry resortowe lub branżowe mogą być tworzone wyłącznie jako rejestry wtórne lub pochodne [Dygaszewicz, Chromicka].

Krytyka takiego założenia związana jest z odrzuceniem koncepcji referencyjnego rejestru na rzecz referencyjnych danych. W interoperacyjnym systemie infrastruktury informacyjnej państwa nie ma miejsca na rejestry w całości referencyjne. Bardziej istotne jest wskazane jest mapowanie miejsc, w których wartości atrybutów (nawet nie rekordy jako całości) uzyskują cechę referencyjności [Stawecki, Gryszczyńska]. Takie podejście powoduje, że pierwszym rozważanym w prezentowanym cyklu zagadnieniem jest referencyjność zasobów informacyjnych w infrastrukturze informacyjnej Państwa.

W – najstarszej w całym cyklu – pracy pt. ***„Pojęcie referencyjności w dyskusji o zasobach informacyjnych państwa"*** (pozycja nr 23 na liście chronologicznej cyklu) podkreśliłem wyraźnie, że dane referencyjne nie powinny być powielane w innych rejestrach, a co najwyżej uzupełniane o dane specyficzne dla danego rejestru pochodnego. Na tej zasadzie dane referencyjne ze zbioru PESEL nie powinny być powielane w innych rejestrach osobowych. Podanie unikalnej cechy referencyjnej (w tym przypadku numeru PESEL) powinno powodować, że w trakcie czynności rejestrowej dotyczącej rejestru pochodnego konieczne dane z rejestru referencyjnego zostaną „zassane", a następnie uzupełnione o komplementarne dane z rejestru pochodnego.

W celu utrzymania porządku pojęciowego należy uznać, że stosowanie wyrażenia „rejestr referencyjny" jest skrótem myślowym, gdyż referencyjne są *de facto* dane, a nie rejestr jako całość. Architektura rejestru nie musi być referencyjna. Nie zawsze też wszystkim danym z rejestru przyznamy również cechę referencyjności.

Pojęcie „referencyjności danych" jest pojęciem kluczowym w procesie budowania infrastruktury informacyjnej państwa. Bez określenia, jakie dane w ramach tejże infrastruktury będą miały charakter podstawowy i do których z nich będą odnosić się inne zasoby informacyjne mieszczące się w tej infrastrukturze, nie możemy mówić w ogóle o istnieniu czegoś takiego jak wspólna infrastruktura. Zestaw danych publicznych, w których żadnym nie przypisuje się referencyjności jest zbiorem rozproszonym i skrajnie redundantnym

Tezy te – stanowiące wstępne założenie całości cyklu – zaprezentowane zostały już w referacie *„Prawne i organizacyjne aspekty neutralności technologicznej i interoperacyjności w Polsce"* wygłoszonym podczas konferencji naukowej *„Informatyzacja administracji publicznej"* zorganizowanej w Sejmie RP w 2004 r. (pozycja 366. na liście II.I) w wykazie dorobku habilitacyjnego) i były rozwijane w kolejnych wykładach konferencyjnych (szczególnie w latach 2009-2012) np. podczas seminarium z cyklu *„Problemy badawcze i projektowe informatyzacji państwa"* (SGH, Uniwersytet Warszawski, WAT, Warszawa 2009 – II.I) poz. 323), zebrania naukowego Instytutu Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego (Kraków 2012 – II.I) poz. 265), IX dorocznej konferencji Polskiej Platformy Bezpieczeństwa Wewnętrznego (Będlewo k. Poznania 2012 – II.I) poz. 222) oraz podczas konferencji *„Co Państwo wie o Tobie ?"* zorganizowanej w ramach obchodów Europejskiego Dniach Ochrony Danych Osobowych 2012 (Warszawa – II.I) poz. 279).

3. Wszechobecność danych. Danetyzacja przestrzeni prawnej

O ile w klasycznej nauce o infrastrukturze informacyjnej państwa rejestry publiczne odgrywają kluczową rolę, wręcz monopolizując całe myślenie o „wiedzy Państwa o samym sobie" [Stawecki, Oleński], o tyle w nowej literaturze przedmiotu coraz częściej odchodzi się od regulowania rejestrów na rzecz prawnych i prawniczych zmagań z danetyzacją rzeczywistości, czyli z fenomenem kwantyfikowania i przekładania na dane wszelkich elementów rzeczywistości, tak by móc poddać je agregowaniu i algorytmizacji [Mayer-Schonberger, Cukier]. Efektem danetyzacji jest skwantyfikowanie otoczenia człowieka – w tym prawa i klasycznych instytucji ekonomicznych – sprofilowanie i postępująca inwigilacja prowadząca do utraty prywatności [Litwiński, Mednis, Fajgielski]. Jednocześnie mamy do czynienia z fetyszyzacją danych i reifikacją rzeczywistości społecznej. Dane które są traktowane jako „opis" obiektywnej rzeczywistości, są w istocie konstruowane w nie zawsze oczywisty – nawet dla twórcy algorytmu – sposób.

Dla zilustrowania praktycznych skutków tego procesu wybrałem do opisu w ramach cyklu trzy – na pozór odległe od siebie – obszary transformacji danetyzacyjnej i postępujących za nią zmian prawnych:

a) elektronizacja dokumentów wykorzystywanych w obrocie morskim i tworzenie platform przetwarzania danych na potrzeby tego sektora (*eMaritime*),
b) przetwarzanie danych biometrycznych na potrzeby stosunków pracodawca-pracownik oraz
c) inteligentne liczniki energii i inteligentne sieci energetyczne (*smart metering* i *smart grid*).

W pierwszej z zaprezentowanych sfer zainteresowań szczególnie istotna dla prowadzonych rozważań była ocena przystosowania klasycznej regulacji z zakresu prawa morskiego do zmian widocznych w praktyce danetyzującego się rynku oraz uwagi *de lege ferenda* [Dragun-Gertner, Czernis]. Główną rolę w prezentacji wyników tych badań przyznaję dwóm pozycjom omawianego cyklu przygotowanym we współautorstwie z moją żoną Iwoną Zużewicz-Wiewiórowską (adiunktem w Katedrze Prawa Morskiego mojej *Alma Mater*):

a) ***„Proces przetwarzania danych z dokumentów elektronicznych w systemach teleinformatycznych e-Maritime"***, „Prawo Morskie", T. 30, 2014 (pozycja nr 9 na liście chronologicznej cyklu) oraz

b) ***„Konosament a blockchain. Możliwości wykorzystania technologii rozproszonego rejestru dla celów 'elektronicznego indosu' przy przenoszeniu praw z papierów wartościowych na zlecenie"*** stanowiącej rozdział pracy *„Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane"*, Warszawa 2019 (pozycja nr 1 na liście chronologicznej cyklu).

Wyniki badań prezentowane w publikacjach były również podstawą dla referatów wygłoszonych podczas posiedzenia Komisji Prawa Morskiego Polskiej Akademii Nauk (Gdańsk 2013 – II.I) poz. 159) oraz dwóch wykładów konferencyjnych podczas VIII Ogólnopolskiej Konferencji Prawa Morskiego pt. *„Przewóz ładunku drogą morską"* (Gdańsk 2019 – II.I) poz. 1) i V Forum Prawa Mediów Elektronicznych (Opole 2019 – II.I) poz. 2).

W drugim omawianym obszarze – biometrii – założenia zaprezentowane podczas wykładu wprowadzającego do panelu *"Biometrics"* podczas 34. Międzynarodowej Konferencji Rzeczników Ochrony Prywatności "*Privacy and Technology in Balance*" (Punta del Este, Urugwaj 2012 – II.I) poz. 232) zostały przedstawione w – stanowiącej część cyklu – pracy pt. ***„Prawna ochrona danych biometrycznych w systemach teleinformatycznych pracodawcy. Cele przetwarzania a zakres ochrony"***, będącej rozdziałem książki *„Ochrona danych osobowych podmiotów objętych prawem pracy i prawem ubezpieczeń społecznych. Stan obecny i perspektywy zmian*, Warszawa 2012 (pozycja nr 19 na liście chronologicznej cyklu) oraz podczas konferencji w Warszawie (2012 i 2011 r. – II.I) poz. 256 i 282) i w Moskwie (2011 – II.I) poz. 291).

Trzeci obszar w którym prowadziłem badania – bardzo ciekawym i nieoczywistym z punktu widzenia prawnego – była danetyzacja w inteligentnych sieciach energetycznych, a w szczególności rola danych z inteligentnych liczników pomiaru zużycia energii w opisywaniu środowiska życia człowieka i tworzeniu infrastrktury danych, które mimo, że z zasady nie są danymi osobowymi, mogą łatwo stać się zdatne do przywiązania do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W tym zakresie do cyklu włączyłem opracowanie ***„Prawo do prywatności w systemie inteligentnych sieci" opublikowane*** *w* „Monitorze Prawniczym" (pozycja nr 12 na liście chronologicznej cyklu), którego główne tezy prezentowane były i rozwijane w podczas wykładów na konferencjach w Brukseli (2018 – II.I) poz. 24; 2012 – II.I) poz. 280), Sofii (2018 – II.I) poz. 21) i w Warszawie (2014 – II.I) poz. 117; 2013– II.I) poz. 176, 177, 202; 2012 – II.I) poz. 211, 221, 230, 251, 260 i 261)).

Podsumowanie rozważań o cesze nieoznaczoności informacji, która związana jest z kontekstową naturą informacji, stanowi publikacja ***„Kwanty informacji o osobie. Prawne aspekty przetwarzania danych o osobach i 'obiektach' pochodzących z rozproszonych zbiorów"***, Warszawa 2013 (pozycja nr 10 na liście chronologicznej cyklu) będąca pokłosiem dyskusji prowadzonej podczas konferencji pt. *„Nowoczesne technologie w procesie karnym i czynnościach wykrywczych a prawa i wolności obywatelskie"* zorganizowanej przez Sąd Najwyższy RP oraz Polską Platformę Bezpieczeństwa

Wewnętrznego przy współpracy Helsińskiej Fundacji Praw Człowieka w Warszawie (2012 – II.I) poz. 239). Temat danetyzacji oraz interoperacyjności semantycznej (omówionej wstępnie w podręczniku „Informatyka prawnicza ...") był również kanwą wystąpień na konferencjach naukowych w Saragossie (2010 – II.I) poz. 308), na Helu (2013 – II.I) 173), w Warszawie (UKSW 2013 – II.I) poz. 187; INP PAN 2012 – II.I) poz. 219; PIU 2010 – II.I) poz. 306; MSWiA 2009 – II.I) poz. 316; SGH 2008 – II.I) poz. 337), Poznaniu (2010 – II.I) poz. 304) oraz w Stalowej Woli – II.I) poz. 305).

4. Wyniki operacji na dużych zasobach danych

W centrum rozważań prezentowanego cyklu znalazły się zagadnienia informacji wyjściowej w procesie przetwarzania dużych zasobów informacyjnych (*Big Data*) traktowanych jako zasoby informacji publicznych. Prezentuję w tym momencie tezę, że przyjmując, iż dane z rejestrów publicznych stanowią informację publiczną i o ile jawność formalna rejestru nie została ograniczona należy mieć świadomość, że dane osobowe z rejestrów publicznych będą ze sobą łączone w dowolny dla administratora sposób. Należy więc pogodzić, się z tym że – przykładowo – dane z ksiąg wieczystych ujawnianych w systemach teleinformatycznych dla zachowania zasad bezpieczeństwa obrotu, będą łączone z danymi z dowolnych rejestrów publicznych, w których ujawniono obiekty przestrzenne (w rozumieniu ustawy. o infrastrukturze informacji przestrzennej), danymi dotyczącymi spraw zagospodarowania przestrzennego prezentowanymi dla celów tworzenia miejscowych planów zagospodarowania przestrzennego, danymi z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, danymi z krajowych rejestrów urzędowych w rozumieniu przepisów o statystyce publicznej (np. REGON, TERYT), czy publicznie dostępnymi danymi z ofert przygotowanych na podstawie przepisów o handlu wierzytelnościami.

Chcąc sprofilować osobę fizyczną, będzie się tą wiedzę uzupełniać danymi z oświadczeń majątkowych składanych przez urzędników publicznych i członków władz publicznych oraz – przede wszystkim – z pozostającymi w gestii danego podmiotu danymi przetwarzanymi z zachowaniem odpowiednich podstaw prawnych a dotyczących jego klientów lub potencjalnych klientów.

Nie ma wątpliwości, że informacja publiczna będzie tym samym wykorzystywana – z użyciem nowej podstawy prawnej formułowanej w prawie do ponownego wykorzystania informacji publicznej – do tworzenia profilu osobowego osoby fizycznej, czyli „automatycznej techniki przetwarzania danych polegającej na przypisaniu danej osobie 'profilu' w celu podejmowania dotyczących jej decyzji bądź analizy lub przewidywania jej preferencji zachowań i postaw". Co więcej takie profile będą miały tak charakter tzw. „profili predykcyjnych" (tworzone w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie w szczególności poprzez uzupełnianie informacji publicznej o monitorowanie odwiedzanych stron oraz reklam, które użytkownik

wyświetla, lub na które klika) jak i tzw. „profili jawnych" (tworzonych na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą).

Na ile taki scenariusz jest praktycznie wykonalny oceniam w dwóch publikacjach włączonych do cyklu:

a) ***„Ponowne przetwarzanie informacji publicznej zawierającej dane osobowe"*** zawartej w książce poświęconej pamięci prof. J. Górzyńskiej, Warszawa 2013 (pozycja nr 11 na liście chronologicznej cyklu) oraz

b) ***„Ochrona prywatności jako ograniczenie prawa do ponownego przetwarzania informacji publicznej"*** z księgi jubileuszowej promotora mojej pracy doktorskiej prof. A. Pułło (pozycja nr 8 na liście chronologicznej cyklu).

Tezy z obu publikacji stały się podstawą dla konstrukcji wykładu podczas konferencji naukowej w FitzWilliam College Uniwersytetu Cambridge (2012 – II.I) poz. 243).

---

5. Profile osobowe a zrównoważenie przetwarzania informacji

Ponieważ wielkoskalowe przetwarzanie danych pochodzących z danetyzowanego otoczenia człowieka prowadzi do tworzenie profili osobowych, zagadnienie to stało się tematem kolejnej części cyklu, na którą składają się dwie zbliżonych do siebie treściowo publikacje:

a) ***"Personal Profiling Based on Generally Accessible Data"***, Sofia 2012 (pozycja nr 20 na liście chronologicznej cyklu) oraz

b) ***„Profilowanie osób na podstawie ogólnodostępnych danych"***, Warszawa 2013 (pozycja nr 13 na liście chronologicznej cyklu)

Tak rozumiane profilowanie i jego ograniczenia były wielokrotnie omawiane przez mnie podczas konferencji naukowych. Do najważniejszych zaliczam wystąpienia z Brukseli (2018 – II.I) poz. 30), Sofii (2018 – II.I) poz. 36), Moskwy (2013 – II.I) poz. 155) i Warszawy (2013 – II.I) poz. 175).

6. Rola Internetu rzeczy

Bardzo duża część prowadzonych przeze mnie w ostatnich latach badań poświęcona była zagadnieniom Internetu rzeczy (IoT), gdyż wdrożenie w praktyce idei IoT prowadzi nie tylko do skokowego zwiększenia ilości dostępnych w procesie danetyzacji danych, ale skłoniło też „architektów" rozwiązań informacyjnych do szerszego otwarcia na zasoby gromadzone przez podmioty spoza administracji publicznej, przy jednoczesnym zezwoleniu na przetwarzanie coraz szerszych gamy informacji pochodzącej od administracji publicznej. Ponieważ szczególnie atrakcyjnym środowiskiem działania IoT dla osób opisujących rolę zdanetyzowanje informacji publicznej się inteligentne miasto (*smart city*), ten właśnie fenomen stał się przedmiotem badań w kolejnej części cyklu tj. w publikacji pt. ***„Dane osobowe w inteligentnym mieście korzystającym z rozwiązań Internetu rzeczy"*** z książki *„Internet rzeczy bezpieczeństwo w smart city"*, Warszawa 2015 (pozycja nr 7 na liście chronologicznej cyklu).

Wychodzę w niej z założenia, że inteligentne miasto XXI w. nie jest jednolitą strukturą stworzoną przez jednego architekta. Nie jest nawet zespołem systemów zarządzanych centralnie przez centrum koordynacyjne na poziomie miasta, aglomeracji czy konurbacji. Jest to zespół z zasady otwartych systemów informacyjnych, które umożliwiają dynamiczne dołączanie do architektury inteligentnego miasta nowych komponentów. Część z systemów pozostaje zamknięta i dostępna jedynie dla głównych twórców danego kompleksu *smart city*, lecz z założenia należy przyjmować, że i te systemy dążyć będą w najbliższej przyszłości do większej otwartości. Dodatkowo wszystkie systemy inteligentnego miasta, by przejawiać rzeczywistą „inteligencję" muszą stale reagować na zmieniające się otoczenie. To w naturalny sposób kieruje nas do uznania, że nowoczesne inteligentne miast musi z zasady opierać się na infrastrukturze Internetu rzeczy.

Internet rzeczy można zdefiniować jako globalną infrastrukturę, w której przedmioty (rzeczy) jako takie lub połączone w jakikolwiek sposób z innymi przedmiotami lub osobami, otrzymują unikalne identyfikatory oraz są w stanie przekazywać dane i współdziałać z innymi systemami wykorzystując możliwości współpracy. IoT ewoluuje w zależności od szybkości i głębokości konwergencji technologii telekomunikacyjnych, systemów elektromechanicznych, mocy obliczeniowych serwerów, przetwarzania w chmurze oraz Internetu. W tym kontekście „rzeczy" definiuje się jako obiekty rzeczywiste lub wirtualne, które istnieją i poruszają się w czasie i przestrzeni oraz mogą być zidentyfikowane przez przypisane im numery identyfikacyjne, nazwy lub adresy lokalizacji . Nieco prostszym językiem IoT definiuje się jako zespół rozwiązań umożliwiający ludziom i rzeczom łączenie się w dowolnym czasie i miejscu z czymkolwiek lub kimkolwiek, w idealnym świecie czyniąc to dowolną drogą lub siecią przy użyciu dowolnej usługi .

Internet rzeczy, obejmujący biliony połączonych urządzeń, jest w stanie przechowywać wszelkiego rodzaje dane (takie jak temperatura, wilgotność, nagrania wideo, ruch, tętno). Podczas, gdy istniejące urządzenia mierzą dane typowe dla środowiska, nowe urządzenia skupiają się bardziej na obserwacji zwyczajów użytkowników. Systemy tworzące IoT lub korzystające z jego zasobów na potrzeby inteligentnego miasta mogą więc przetwarzać dane, które uznawać będziemy za dane osobowe. Internet rzeczy łączy zarówno urządzenia istniejące dotychczas a wyposażone dodatkowo w chip RFID zapewniający im bytność w Internecie, jak i urządzenia utworzone specjalnie w celu połączenia z Internetem (na stałe lub jedynie okazjonalnie).

Temat rozwijany również we wykładzie otwierającym sesję *„Noc architektów. Internet rzeczy - czyli czas na podział władzy"* podczas XXII Forum Teleinformatyki w Warszawie (2016), którego nagranie jest w całości dostępne w sieci (zasoby *Youtube*) oraz w licznych wykładach na konferencjach naukowych, z których za najważniejsze uważam wykłady w Krakowie (2016 – II.I) poz. 92) i w Parlamencie Europejskim (2017 – II.I) poz. 55), Warszawie (2015 – II.I) poz. 109) i w Gdańsku (2014 – II.I) poz. 120).

7. Przetwarzanie w chmurze

Oczywistą kontynuacją rozważań jest ocena wybranych zagadnień prawnych stosowania modelu chmury (niepoprawnie nazywanego „chmurą obliczeniową") w administracji publicznej. Oceny takiej dokonałem w trzech podobnych do siebie publikacjach – tak jak w przypadku profilowania – wydanych w języku angielskim i polskim. Obok opublikowanego w Bułgarii artykułu ***"Legal Aspects of e-Governmental Clouds"***, Sofia 2013 (pozycja nr 15 na liście chronologicznej cyklu) oraz pokonferencyjnej publikacji w ***"Privacy and the Liability of Intermediary Service Provider in the Clouds. E-Governmental Aspects"*** wydanej przez węgierskiego publikatora dzienników urzędowych, Budapeszt 2011 (pozycja nr 21 na liście chronologicznej cyklu), w kolejnej książce z cyklu *„Bezpieczeństw w Internecie"* ukazał się poświecony temu zagadnieniu rozdział pt. ***„Prawne aspekty udostępniania usług administracji publicznej w modelu chmury***, Warszawa 2013 (pozycja nr 14 na liście chronologicznej cyklu).

Wskazania w zakresie zrównoważonego przetwarzania danych w chmurze przez administrację publiczną sformułowane zostały jako dekalog dla instytucji publicznej (nazwany niekiedy *„Dekalogiem chmuroluba"*) i przedstawiane były podczas wystąpień na konferencjach naukowych w Bukareszcie (2016 – II.I) poz. 77), Belgradzie (2013– II.I) poz. 199), Kijowie (2012 – II.I) poz. 249), Luksemburgu (2013 – II.I) poz. 161), Meksyku (2011 – II.I) poz. 290), Helu (2013 – II.I) poz. 172), Poznaniu (2011 – II.I) poz. 285), Warszawie (2014 – II.I) poz. 153; 2013 – II.I) poz. 184; 2012 – II.I) poz. 229, 234 i 278; 2011– II.I) poz. 292, 293 i 301), Wrocławiu (2012 – II.I) poz. 227) oraz w serii spotkań z

praktykami informatyki administracyjnej w Puszczykowie (2013 – II.I) poz. 191), Wilkasach (2013 – II.I) poz. 197), Spale (2013 – II.I) poz. 213) i Jachrance (2011 – II.I) poz. 295).

8. Świt sztucznej inteligencji

Osobnym nurtem rozważań związanych z danetyzacją oraz ze zrównoważeniem przetwarzania informacji o osobach jest kwestia wykorzystania w procesie przetwarzania bytów sztucznie inteligentnych lub co najmniej rozbudowanych algorytmów opartych o głębokie uczenie (*deep learning*) [Przegalińska]. Te zagadnienia będą stanowiły *clue* moich przyszłych badań, ale już dziś są obecne w prezentowanym cyklu w postaci przygotowanego wspólnie z drem Grzegorzem Sibigą z INP PAN opracowania pt. ***„Automatyzacja rozstrzygnięć i innych czynności w sprawach indywidualnych załatwianych przez organ administracji publicznej"*** zamieszczonego w pracy zbiorowej pt. *„Informatyzacja postępowania sądowego i administracji publicznej"* z 2010 r. (pozycja nr 22 na liście chronologicznej cyklu).

Jest w obecnej chwili jedyna moja publikacja dotycząca tego aspektu zrównoważonego przetwarzania informacji, choć prawnicze zastosowania sztucznej inteligencji oraz możliwość prawnej regulacji przetwarzania danych (w tym danych osobowych) były również tematami moich wystąpień konferencyjnych. Do najważniejszych z nich zaliczam referat: pt. *„Komputacyjne modele prawa. Dyskusja nad zastosowaniem metod sztucznej inteligencji we wnioskowaniach prawniczych"* wygłoszony podczas XX Zjazdu Katedr Teorii i Filozofii Prawa w 2012 r. w Łodzi (2012 – II.I) poz. 295), prezentację *"Data Protection Issues in Artificial Intelligence & High Performing Computing"* w Parlamencie Europejskim (2018 – II.I) poz. 295), wykład *"Artificial Intelligence in humanitarian actions"* podczas warsztatów *"From Privacy to Ethics: Misuse, Missed Use, and the Public Good"* podczas 40. Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności odbywającej się w Brukseli (2018 – II.I) poz. 15), wykład pt. *"Ethics by Design in Artificial Intelligence?"* wygłoszony podczas wcześniejszej o rok edycji tej samej Konferencji zorganizowanej w Hongkongu (2017 – II.I) poz. 46) oraz dwa wykłady z 2017 r. wygłoszone na Uniwersytecie w Cambridge:

a) *"Artificial inteligence in legal profession"* (British Law Centre, Queens' College – II.I) poz. 50) i
b) *"Fair and lawful processing: Understanding the logic behind Artificial Intelligence algorithms"* (Privacy Laws & Business, St. John's College– II.I) poz. 52).

9. Ochrona danych osobowych jako droga ku zrównoważeniu przetwarzania

Proponowaną drogą rozwiązania jest prawidłowe wykorzystanie narzędzi oferowanych przez zreformowane europejskie prawo o ochronie danych osobowych (RODO). Zagadnieniu roli reformy ochrony danych osobowych w Unii Europejskiej poświęciłem trzy publikacje włączone do cyklu:

a) ***„Nowe ramy ochrony danych osobowych w Unii Europejskiej***, publikowana w 2012 r. w „Monitorze Prawniczym" (pozycja nr 17 na liście chronologicznej cyklu);

b) ***„Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa***, z kwartalnika „Krajowa Rada Sądownictwa" z 2013 r. (pozycja nr 16 na liście chronologicznej cyklu) oraz

c) ***„Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych",*** ze specjalnego numeru „Europejskiego Przeglądu Sądowego" z 2017 r. poświęconego RODO (pozycja nr 2 na liście chronologicznej cyklu).

Do cyklu nie włączyłem tegorocznej publikacji: *„Wpływ RODO na rozwój prawa ochrony danych osobowych poza Unią Europejską"* [w:] G. Szpor [red.:] *„Internet. Przetwarzanie danych osobowych"*, Warszawa 2019, ss. 33; gdyż oficjalnie ukaże się ona na rynku dopiero w maju 2019 r., czyli po złożeniu niniejszego wniosku. Jest ona jednak naturalnym przedłużeniem wcześniejszych rozważań.

10. Szczególne uprawnienia państwa a gwarancje ochrany godności człowieka

Ostatnie dwa lata zostały w dużej mierze poświęcone zostały na badanie gwarancji ochrony praw podstawowych przy dopuszczalnych formach ingerencji w prywatność, których nie można traktować jako naruszenia zasad zrównoważonego przetwarzania. Szczególna rola organów ścigania i wymiaru sprawiedliwości w sprawach karnych oraz zwiększone uprawnienia służb specjalnych zawsze stanowiły wyzwanie przy określaniu wszelkich form równoważenia siły instytucji państwowych Efektem tych prac są dwa większe opracowania włączone do cyklu:

a) angielskojęzyczna praca ***"Surveillance for public security purposes. Four pillars of acceptable interference with the fundamental right to privacy"*** wydana w przgotowanym przez Uniwersytet w Gandawie o redagowanym przez prof. G.Vermeulen, z którym miałem okazję współpracować, przez kilka ostatnich lat opracowaniu *"Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data"*, Antwerpia-Apeldoorn-Portland 2017 (pozycja nr 3 na liście chronologicznej cyklu) oraz

b) adresowana w większym stopniu do polskiego czytelnika podobna publikacja pt. *„Inwigilacja w celu zapewnienia bezpieczeństwa publicznego. Cztery filary dopuszczalnej ingerencji w prawo do prywatności”*, zamieszczona w 24. Tomie „Disputatio. Przegląd Naukowy” (pozycja nr 4 na liście chronologicznej cyklu).

Poza konferencją w Gandawie, przed którą wydana został publikacja redagowana przez prof. G. Vermeulena (II.I) poz. 39) tematy te stanowiły podstawę moich wystąpień m.in. na konferencjach naukowych organizowanych przez Akademię Prawa Europejskiego (ERA) i Sieć Ekspertów ds. Ochrony Danych EUROPOLu w Hadze (2018 – II.I) poz. 10), *Fédération des Barreaux d'Europe* (FBE) w Warszawie (2018 – II.I) poz. 18), *European Digital Rights* (EDRi) w Brukseli (2018 – II.I) poz. 33), Naukowe Centrum Prawno-Informatyczne na UKSW w Warszawie (2016 – II.I) poz. 87), Naczelną Radą Adwokacką w Warszawie (2016 – II.I) poz. 88), Prokuratora Generalnego i Trybunał Konstytucyjny w Warszawie (2013 – II.I) poz. 209), Europejską Agencję Bezpieczeństwa Sieci ENISA, DG CONNECT i Uniwersytet Wiedeński w Wiedniu (2017 – II.I) poz. 57) oraz *Chatham House* w Londynie (2016 – II.I) poz. 86)

Innym szczególnym przypadkiem swoistego hamowania kreatywności prawodawcy europejskiego i ustawodawców krajowych jest dyskusja nt wprowadzenia do praw i praktyki sytemów wymiany danych PNR, o któ®ych piszemy z I. Zużewicz-Wiewiórowską w artykule pt. ***„Re-use of Maritime Passengers' PNR Data for Public Security Purposes”***, w czasopiśmie „Prawo Morskie” z 2017r. (pozycja nr 5 na liście chronologicznej cyklu).

---

11. Ochrona prywatności wbudowana w przetwarzanie danych

Podsumowaniem rozważań o możliwości równoważenia rozdział ***„Privacy by Design jako paradygmat ochrony prywatności”*** w książce *„Internet. Prawno-informatyczne problemy sieci, portali i e-usług”*, Warszawa 2012, którą współredagowałem jako całość wraz z prof. G. Szpor, z UKSW. Zagadnienie to stanowiło również treść moich wystąpień konferencyjnych w Wiedniu i Barcelonie (2017 i 2018 – II.I) poz. 57 oraz 19), zaś drogi realizacji zasady PbD były częścią moich rozważań podczas sesji plenarnej 9. Warsztatów Internet Privacy Engineering Network (IPEN) w Brukseli (2019 – II.I) poz. 6). Uzupełnieniem tej linii wykładów było wystąpienie pt. "*Compliant or/and Accountable in Privacy by Design Environment*" podczas seminarium pt. "*European Parliament Data Protection Day. Managing accountability and compliance in the Reform Era*" zorganizowanego przez Parlament Europejski w Brukseli (2017 – II.I) poz. 54).

c) Wykorzystanie wyników prac badawczych

Dzięki możliwości łączenia pracy naukowej na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego z pracą w administracji publicznej - tak w Ministerstwie Spraw Wewnętrznych i Administracji jak i od 2010 r. pełniąc funkcję Generalnego Inspektora Ochrony Danych Osobowych i w końcu od 2014 r. jako Zastępca Europejskiego Inspektora Ochrony Danych miałem możliwość na bieżąco wprowadzać niektóre z rozwiązań proponowanych w pracach naukowych do dyskusji dotyczącej zmian w prawie bądź implementacji już istniejących rozwiązań prawnych. Najbardziej charakterystycznym przykładem takiego wpływu jest rozwinięcie koncepcji referencyjności danych infrastrukturze informacyjnej państwa, która została wykorzystana przy tworzeniu Krajowych Ram Interoperacyjności oraz przetworzeniu infrastruktury rejestrów publicznych na potrzeby realizowanych przez Ministerstwo Spraw Wewnętrznych i Ministerstwo Cyfryzacji projektów informatycznych.

Koncepcja zrównoważonego przetwarzania informacji stała się podstawą wystąpień GIODO kierowanych do legislatorów w trakcie prac nad zmianą ustawy o dostępie do informacji publicznej, statystyce publicznej oraz o poszczególnych rejestrach publicznych (ze szczególnym uwzględnieniem Krajowego Rejestru Sądowego oraz elektronicznych ksiąg wieczystych). Poszczególne zagadnienia dotyczące profilowania oraz przenoszenia danych były wykorzystywane przy przygotowywaniu opinii GIODO oraz EDPS w trakcie prac nad reformą prawa ochrony danych osobowych w Unii Europejskiej oraz nad harmonizacją wprowadzania RODO do porządku prawnego państw członkowskich.

5. Omówienie pozostałych osiągnięć naukowo - badawczych (artystycznych).

Stopień doktora nauk prawnych otrzymałem po obronie pracy doktorskiej z zakresu amerykańskiego prawa konstytucyjnego w Wydziale Prawa i Administracji Uniwersytetu Gdańskiego. Ta tematyka badawcza nie była jednak kontynuowana przeze mnie po 2000 r. z drobnym wyjątkiem jednej recenzji książki opublikowanej w „Przeglądzie Sejmowym".

Od 1996 byłem zawodowo – poza swoją *Alma Mater* – związany z zagadnieniami informatyki prawniczej i prawa nowych technologii informacyjnych, co spowodowało, że po uzyskaniu stopnia doktora całość moich zainteresowań naukowych skierowana była na obszar przetwarzania informacji oraz prawnej regulacji nowych technologii komunikacyjnych.

W latach 2006-2010 pracowałem w administracji rządowej w dziale informatyzacja - przekazanym wówczas do zarządzania Ministrowi Spraw Wewnętrznych i Administracji. Umożliwiło mi to łączenie zainteresowań naukowych z praktyką budowy infrastruktury informacyjnej państwa. Pełniąc funkcję doradcy w gabinecie politycznym ministra odpowiedzialnego za dział informatyzacji, a później będąc dyrektorem Departamentu Informatyzacji Ministerstwa Spraw Wewnętrznych i Administracji, prowadziłem jednocześnie prace naukowe z zakresu informatyzacji administracji publicznej oraz prawa komputerowego oraz realizowałem w praktyce znaczącą część proponowanych przez siebie rozwiązań *de lege ferenda*.

Po 2010 r. w związku zawodowym zaangażowaniem się w prace związane z reformą polskiego i europejskiego prawa ochrony danych osobowych moje zainteresowania naukowe ewoluowały również w tą stronę, obejmując szerokie spektrum zagadnień związanych z ochroną prywatności w Polsce, w Europie i w skali globalnej. W latach 2010-2014 sprawowałem funkcję Generalnego Inspektora Ochrony Danych Osobowych (GIODO), a w grudniu 2014 r. zostałem wybrany wspólną decyzją Parlamentu Europejskiego i Rady Unii Europejskiej na stanowisko Zastępcy Europejskiego Inspektora Ochrony Danych (EDPS /EIOD) i od tego czasu kontynuuje pracę zawodową w Brukseli - w strukturach instytucji unijnych - jednocześnie prowadząc prace naukowe i dydaktyczne na Wydziale Prawa i Administracji Uniwersytetu Gdańskiego.

Moja praca naukowa obejmowała pięć głównych obszarów badawczych, które nie znalazły się w ramach cyklu proponowanego do oceny postępowania charakteru habilitacyjnym

Prawo Internetu

Pierwszym z nich były ogólne zagadnienia prawa nowych technologii ze szczególnym uwzględnieniem regulacji jednolitego rynku cyfrowego oraz prawnych aspektów komunikacji elektronicznej pomiędzy podmiotami, działającymi w różnych rolach na tymże rynku oraz pomiędzy podmiotami wykorzystującym nowe techniki komunikacyjne do działań niezwiązanych z działalnością zawodową lub zarobkową. Tą część mojej pracy naukowej najlepiej ilustruje opracowanie z 2012 roku:

1. *Internet. Prawno-informatyczne problemy sieci, portali i e-usług* [współredakcja:] G. Szpor, C.H.Beck, Warszawa 2012, ss. 389, ISBN 978-83-255-3908-5; e-book 978-83-255-3793-7.

Ochrona danych osobowych

W czasie pełnienia funkcji Generalnego Inspektora Ochrony Danych Osobowych oraz Zastępcy Europejskiego Inspektora Ochrony Danych *gross* mojej pracy naukowej było – z oczywistych względów – związane z problematyką reformy prawa ochrony danych osobowych. Poza publikacjami wchodzącymi w skład cyklu pragnę zwrócić uwagę na poniższe publikacje:

2. *Wpływ RODO na rozwój prawa ochrony danych osobowych poza Unią Europejską* [w:] G. Szpor [re.:] *Internet. Przetwarzanie danych osobowych*, Warszawa 2019, ss. 33; [w druku]
3. *15 years of personal data protection in Poland and in Central Europe* [w:] F. Giuseppe [red.:] *Tutela dei dati personali in Italia 15 anni dopo. Tempo di bilanci e di bilanciamenti*, Egea, Mediolan 2012, s. 11, ISBN 978-88-238-4314-1.

Świadczenie usług drogą elektroniczną

W pierwszej fazie swojej pracy naukowej nad zagadnieniami prawnymi komunikacji elektronicznej większą uwagę poświęcałem prawnej regulacji handlu elektronicznego. Z tego czasu pochodzą moje opracowania dotyczące świadczenia usług drogą elektroniczną (*e-commerce)*, a w szczególności kwestii ewentualnego rozszerzenia ograniczeń odpowiedzialności podmiotów świadczących usługi drogą elektroniczną. W artykule pt.:

4. *Wyłączenie odpowiedzialności usługodawcy świadczącego usługi drogą elektroniczną za niektóre rodzaje usług (uwagi de lege ferenda)*, Gdańskie Studia Prawnicze XXI, Gdańsk 2009 s. 199-212,

proponowałem rozwiązania, umożliwiające uzupełnienie klasycznego katalogu ograniczeń odpowiedzialności wynikających z dyrektywy *e-commerce* – to jest *hostingu, cashingu* i *mere conduit* o dodatkowe wyłączenia i ograniczenia oraz wysuwałem wnioski dotyczące tzw. procedur *notice and take down.*

Informacja prawna

Zagadnieniami stale obecnymi w pracach naukowych Zakładu Informatyki Prawniczej Wydziału Prawa i Administracji Uniwersytetu Gdańskiego, z którym związany jestem od 2003 r. i której to jednostki (jeszcze wówczas pod nazwą Pracownia Informatyki Prawniczej) byłem w latach 2003-2010 kierownikiem, są zagadnienia związane z tworzeniem systemów informacji prawnej oraz z teoretycznym i praktycznymi problemami wykorzystywania tychże systemów w procesie wykładni prawa. Poza publikacjami podręcznikowymi skierowanymi do studentów kierunków: prawo i administracji oraz do urzędników publicznych i prawników, wykonujących klasyczne zawody prawnicze, byłem zaangażowany w tworzenie opracowań naukowych, dotyczących roli systemów informacji prawnej oraz niebezpieczeństw związanych z nadmiernym zaufaniem, jakim systemy te darzą użytkownicy. W ramach tych prac byłem autorem następujących publikacji:

5. *Elektroniczna publikacja prawa. Problemy techniki prawodawczej*, „Prawo Nowych Technologii", Nr 1 z 2008 r., s. 71-81;
6. *Europejska informacja prawna w Internecie* [w:] Z. Brodecki [red.:] *Regiony*, LexisNexis, Warszawa 2005, s. 17, ISBN 83-7334-422-5;

7. *Zagrożenia związane z zarządzaniem informacją prawną i prawniczą w środowisku elektronicznym* [w:] H. Ganinska [red.:] *Informacja dla nauki a świat zasobów cyfrowych*, Biblioteka Główna Politechniki Poznańskiej, Poznań 2008, s. 14, ISBN 83–910677–4–2;
8. *System prawa z perspektywy systemu informacji prawnej* [współautor:] G. Wierczyński, [w:] J. Zajadło [red.:] *Gdańskie Studia Prawnicze. Filozofia dogmatyk prawniczych.* Tom XVIII, Wyd. UG, Gdańsk 2007, ISBN: 1234-4303;

Haking

W pierwszych latach pracy naukowej znaczącą część moich badań poświęcałem zagadnieniom prawnokarnej regulacji cyberprzestępstw - w tym szczególności nie precyzyjnej regulacji tzw. *hakingu,* prowadzącej do niezamierzonej przez ustawodawcę penalizacji działań związanych z tworzeniem i wykorzystywaniem rozwiązań kryptograficznych oraz oprogramowania służącego do przeprowadzania testów penetracyjnych. Rezultaty tych badań zamieściłem m.in. w następujących publikacjach:

9. *Prawnokarne aspekty działań informatycznych. Czy Polskie Towarzystwo Informatyczne jest zorganizowaną grupą przestępczą?* [w:] P. Fuglewicz, J. Nowak [red.:] *Społeczne aspekty informatyki*, Polskie Towarzystwo Informatyczne, Katowice 2009, s. 10, ISBN 978-83-60810-13-2;
10. *Czego nie może posiadać kryptolog ? Odpowiedzialność karna za posiadanie 'narzędzi, komponentów i programów do usuwania skutecznych zabezpieczeń'* [w:] *XI Krajowa Konferencja Zastosowań Kryptografii ENIGMA 2007. Materiały konferencyjne,* Enigma, Warszawa 2007;
11. *Profesjonalny haker. Paradoks odpowiedzialności karnej za czyny związane z ochrona danych i systemów komputerowych* [w:] *Bezpieczeństwo sieci komputerowych a hacking. Internetki V* - materiały z konferencji naukowej, Wyd. UMCS, Lublin 2005, s. 38-47.