# AUTOREFERAT

## Przedstawiający opis dorobku oraz osiągnięć naukowych dr Arwida Mednisa

Niniejszy autoreferat został sporządzony zgodnie z art. 16 i art. 18a ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (tekst jedn. Dz. U. z 2016 r. poz. 882, ze zm.) oraz §12 ust. 2 rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 26 września 2016 r. w sprawie szczegółowego trybu i warunków przeprowadzania czynności w przewodzie doktorskim, w postępowaniu habilitacyjnym oraz w postępowaniu o nadanie tytułu profesora (Dz. U. poz. 1586, ze zm.). Zawiera on opis dorobku i osiągnięć naukowych habilitanta, w szczególności określonych w art. 16 ust. 2 ustawy. Autoreferat został przygotowany zgodnie ze wzorem zamieszczonym na stronie internetowej Centralnej Komisji do Spraw Stopni i Tytułów (http://www.ck.gov.pl/articles/id/47.html).

### 1. Imię i nazwisko.

Arwid Mednis

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

W dniu 20.06.2005 r. uzyskałem stopień doktora nauk prawnych w zakresie prawa. Został on nadany przez Radę Wydziału Prawa i Administracji Uniwersytetu Warszawskiego na podstawie pracy naukowej pt. „Prawo do prywatności a interes publiczny. Studium z aksjologii prawa publicznego", przygotowanej pod opieką naukową prof. UW dr hab. Michała Kuleszy. Recenzentami rozprawy doktorskiej byli prof. dr hab. Marian Zdyb oraz prof. dr hab. Krzysztof Pietrzykowski.

Tytuł zawodowy magistra prawa uzyskałem na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego w dniu 6.10.1989 r. (studia w latach 1983-1989). Moja praca magisterska

dotyczyła plagiatu programu komputerowego i została przygotowana pod kierunkiem prof. dr hab. Jana Błeszyńskiego.

**3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych.**

Na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego jestem zatrudniony od 1.10.1989 roku.

Przebieg zatrudnienia na WPiA UW:

1989-1990 asystent stażysta

1990-1998 asystent

1998-2005 wykładowca

2005-2011 adiunkt

2011-2016 docent

2016 do chwili obecnej starszy wykładowca.

W chwili obecnej jestem zatrudniony na podstawie umowy o pracę na czas nieokreślony w Zakładzie Nauki Administracji w Instytucie Nauk Prawno-administracyjnych na WPiA UW.

**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. 2017 r. poz. 1789):**

***4.1 Tytuł osiągnięcia naukowego***

Jako osiągnięcie naukowe w dyscyplinie prawo w rozumieniu art. 16 ust. 2 ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki, pragnę wskazać monografię:

**Prawo ochrony danych osobowych wobec profilowania osób fizycznych, Presscom, Warszawa 2019, ISBN 978-83-65611-73-4, recenzent wydawniczy: Prof. zw. dr hab. Jacek Jagielski**

### *4.2 Uzasadnienie wyboru tematu pracy i cel rozprawy*

Zajmując się prawem ochrony danych osobowych od wielu lat śledzę nie tylko rozwój regulacji prawnej, ale również zmiany w sposobie wykorzystywania danych osobowych i wynikające z tego nowe zagrożenia dla naszej prywatności i innych praw i wolności obywatelskich. Sfera technologii informatycznych i praw obywatelskich są ściśle ze sobą związane a prawo ochrony danych osobowych jest tu przykładem szczególnym.

Od czasu pierwszych aktów prawnych z tego zakresu, prawo ochrony danych osobowych ewoluowało próbując odpowiedzieć na nowe wyzwania technologiczne i biznesowe.

Pochodzące z lat 70-tych i 80-tych XX wieku pierwsze krajowe i europejskie regulacje były odpowiedzią na zastosowanie komputerów do przetwarzania informacji. Obawiano się przede wszystkim błędów w elektronicznych bazach danych, a jednocześnie starano się zapewnić jednostce kontrolę nad wykorzystywaniem jej danych osobowych. Ówczesne zagrożenia wynikały w zasadzie wyłącznie z przetwarzania danych przez podmioty publiczne lub ośrodki naukowe, ponieważ do lat 80-tych XX w. tylko one dysponowały odpowiednimi jednostkami obliczeniowymi. Komputery na masową skalę zaczęły trafiać do gospodarstw domowych na przełomie lat 70-tych i 80-tych, stopniowo rosły też możliwości ich wykorzystania, również dla celów przetwarzania danych osobowych. Wraz z rosnącymi możliwościami komputerów i coraz szerszym ich wykorzystaniem rosły zagrożenia dla praw jednostki. Już nie tylko administracja i nauka korzystały z zasobów danych o ludziach, takie zasoby zaczęli tworzyć przedsiębiorcy i osoby prywatne.

W 1981 roku przyjęto pierwszą międzynarodową regulację prawną dotyczącą tego zagadnienia, tj. Konwencję nr 108 Rady Europy o ochronie osób ze względu na przetwarzanie danych osobowych. Stanowiła ona podstawę do rozwoju regulacji krajowych w państwach członkowskich. Jednak przepisy przyjęte w tamtym okresie w poszczególnych państwach różniły się jednak znacznie między sobą. Stąd, w latach 90-tych XX w. podjęto starania w celu ich ujednolicenia, a rezultatem tych starań była Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Dyrektywa określała podstawowe zasady przetwarzania danych osobowych, przesłanki legalności przetwarzania oraz prawa podmiotu danych. Jednym z podstawowych praw było prawo do uzyskania informacji o okolicznościach wykorzystywania danych, umożliwiające kontrolę nad

obiegiem danych osobowych jednostki. Dyrektywa została w Polsce implementowana w postaci ustawy o ochronie danych osobowych z 1997 r.

Przepisy Dyrektywy były tworzone w czasach, gdy nie było jeszcze serwisów społecznościowych a Internet był jedynie systemem stron z informacjami. Tymczasem, rozwój usług świadczonych przez Internet szedł w parze z gromadzeniem coraz większej liczby danych o użytkownikach. Jednocześnie rozwijano narzędzia analityczne, pozwalające na wykorzystanie tych danych w celu zdobycia wiedzy na temat różnych zjawisk, w tym na temat zachowania konsumentów. Gromadzenie danych stało się obecnie tym łatwiejsze, że do Internetu podłącza się coraz więcej urządzeń: samochody, przedmioty codziennego użytku, sprzęt AGD, zabawki, itp. Kilkanaście lat temu pojawiło się określenie *Big data* oznaczające możliwość przetwarzania dużych zbiorów danych (nie tylko osobowych), pochodzących z różnych źródeł i mających różne formy i formaty (pliki tekstowe, zdjęcia, pliki muzyczne, tabele, itd.)

Analityka klasy *Big data* pozwala na coraz dokładniejsze określanie cech konsumentów, przedsiębiorców i obywateli oraz na przewidywanie ich zachowania. Pozytywne rezultaty wykorzystania tego typu narzędzi z jednej strony zachęcają do zbierania coraz większej liczby danych, z drugiej – do rozwijania nowych usług i produktów opartych na profilowaniu osób. Profilowanie polega tu na znalezieniu określonych korelacji pomiędzy różnymi danymi w zbiorze oraz stworzeniu na tej podstawie kategorii osób oraz przypisaniu tym kategoriom odpowiednich cech. Algorytmy profilujące wskazują klientów, którzy są skłonni kupić dany produkt, kojarzą pary w serwisach randkowych, przewidują choroby, preferencje polityczne, wskazują potencjalnych oszustów podatkowych, itp.

Algorytmy dokonują zatem automatycznej klasyfikacji i kategoryzacji osób, a na tej podstawie podejmuje się (zwykle również automatyczne) działania wobec nas jako konsumentów i obywateli. Argument, że narzędzia te są coraz dokładniejsze ma uzasadniać coraz szersze ich zastosowanie, zarówno w sektorze publicznym jak i prywatnym. Ma on również uzasadniać gromadzenie coraz większych ilości danych osobowych, ponieważ im więcej danych tym dokładniejsze określenie korelacji pomiędzy różnymi czynnikami (np. można precyzyjniej określi przyczyny wypadków drogowych). Profilowanie ma swoje dobre strony, ale należy pamiętać, że opiera się na metodach statystycznych i matematycznych i – siłą rzeczy – niesie ze sobą ryzyko błędów. Dotyczy to również profilowania z wykorzystaniem sztucznej inteligencji, ponieważ nadal mamy do czynienia z tzw. słabą sztuczną inteligencją, opartą o metody statystyczne. Jej przewaga nad człowiekiem w niektórych dziedzinach opiera się na

nieporównywalnie większej zdolności szybkiego przetworzenia dużej ilości danych. Maszyna nie myśli jak człowiek, lecz podejmuje decyzje na podstawie określenia prawdopodobieństwa, że dane rozwiązanie jest poprawne.

Mamy do czynienia z profilowaniem bezpośrednim i pośrednim, to pierwsze ma miejsce, gdy próbujemy określić cechy osoby na podstawie danych jej dotyczących, z drugim, gdy cechy te określamy na podstawie danych o innych osobach. W tym drugim przypadku mamy często do czynienia z dużą liczbą danych historycznych oraz modelami predykcyjnymi budowanymi przez analityków. Takie modele tworzone są dla potrzeb administracji (np. profilowanie bezrobotnych, profilowanie podatników), przedsiębiorców (firmy ubezpieczeniowe określają ryzyko ubezpieczeniowe, banki – zdolność kredytową), w internecie oferuje się profile użytkowników w celach marketingowych. Profilowanie wykorzystywane jest w medycynie, wojsku, policji, pomocy społecznej i wielu innych obszarach.

Główne zidentyfikowane przeze mnie zagrożenia w sferze praw i wolności wynikające z tak rozumianego profilowania to: naruszenie prywatności i autonomii woli jednostki, dyskryminacja, manipulowanie ludźmi, a także inne ryzyka, np. takie, że błędy w profilowaniu mogą prowadzić do strat materialnych.

Ryzyko dla prywatności jest oczywiste: dla celów profilowania gromadzi się ogromną liczbę danych. Pozostają one często poza kontrolą podmiotu danych. Jednocześnie, pojawia się problem niedostatecznego zabezpieczenia tych danych, szczególnie w sytuacji, gdy wzrastającej ilości gromadzonych danych nie towarzyszy wzrost nakładów na bezpieczeństwo informatyczne.

Profilowanie może ograniczać autonomię woli jednostki. Jeżeli w wyniku profilowania oferuje nam się towar bądź usługę nie pozostawiając wyboru wówczas autonomia woli może być naruszona. W sieci mamy często do czynienia z pozbawianiem nas prawa wyboru, przymuszaniem nas do zakupu określonych towarów lub usług. Np. wymusza się na klientach płacenie swoją prywatnością. W książce podaję wiele takich przykładów, np. amerykańskiej firmy ubezpieczeniowej, która w 2018 roku ogłosiła, że będzie sprzedawała polisy wyłącznie klientom, którzy przekażą dane o swojej aktywności fizycznej (mieliby ujawniać je w aplikacji lub na stronie www albo udostępniać dane z tzw. trackerów fitnesowych (opasek i zegarków).

Przymusza się nas do pewnych decyzji lub wręcz decyduje za nas bez naszej wiedzy. Osoba kupująca bilet lotniczy online nie ma wiedzy na temat tego, że inne osoby zalogowane w tym samym czasie i zainteresowane biletem na tę samą trasę w tym samym dniu otrzymały niższą

cenę tylko dlatego, że łączyły się z siecią z tańszego urządzenia. Mamy tu więc do czynienia z aspektem autonomii woli, który może zostać naruszony poprzez profilowanie.

Poważnym problemem przy profilowaniu jest ryzyko dyskryminacji i pogłębiania rozmaitych uprzedzeń. Podane w książce przykłady potwierdzają tezę, że część używanych algorytmów pogłębia uprzedzenia istniejące w realnym świecie. Dotyczy to również sfery publicznej (podaję przykłady algorytmów używanych w sądach lub przez policję, powielających uprzedzenia rasowe i in.). Niektóre algorytmy są uznawane za poprawne tak długo jak długo przynoszą zysk.

Profilowanie wykorzystuje się również do manipulowania ludźmi i dezinformacji. Zjawiska te same w sobie nie są oczywiście niczym nowym. Jednak segmentacja odbiorców ze względu na ich cechy z użyciem nowoczesnych narzędzi analitycznych i ogromnych ilości danych pozwala na precyzyjny dobór przekazu dopasowany do cech odbiorcy. Przykładem jest sprawa Cambridge Analytica, która wywołała dyskusje na temat możliwości wykorzystania danych w celu manipulowania zachowaniem ludzi w związku z wyborami prezydenckimi w USA. Według niektórych źródeł skuteczność manipulowania poglądami użytkowników sieci jest jak na razie niewielka, niemniej organy takie jak Europejski Rzecznik Ochrony Danych zalecają już współpracę organów ochrony danych z organami wyborczymi.

Nie bez powodu mówi się o pojęciu bańki informacyjnej. W szerszym obiegu zaczęło ono funkcjonować przy okazji wyborów prezydenckich w USA w 2016 r. Inaczej zwana „bańką filtrującą" (ang. filter buble), polega na użyciu algorytmu filtrującego informacje dostarczane użytkownikowi w sieci w zależności np. od jego lokalizacji, historii wyszukiwania lub innych zidentyfikowanych cech. Działanie algorytmu prowadzi do odizolowania użytkownika od określonych treści, co z kolei może prowadzić do pogłębienia różnic postaw i poglądów, utrudnić porozumienie, umocnić ludzi w ich poglądach.

Profilowanie i podejmowane na jego podstawie zautomatyzowane decyzje mogą prowadzić również do innych negatywnych skutków, np. strat finansowych, itp.

Niezbędne są zatem prawne mechanizmy kontroli powyższych procesów. Temat ten został w polskiej literaturze prawniczej podniesiony w kilku artykułach, nie doczekał się jednak do tej pory pogłębionego omówienia. Profilowanie było już natomiast przedmiotem orzecznictwa i to również w Polsce. Fakt, że nasze życie przenosi się stopniowo do Internetu, a wirtualna rzeczywistość ulega algorytmizacji powoduje moim zdaniem, że będziemy mieli coraz częściej do czynienia ze sprawami tego typu. Wybierając temat kierowałem się przede wszystkim

aktualnością zagadnienia oraz tym, że nie jest ono jeszcze dostatecznie omówione. Literatura jest na etapie identyfikacji zagrożeń jakie profilowanie niesie dla jednostki. Zdecydowałem się więc na analizę profilowania z perspektywy praw osób profilowanych.

Profilowanie osób opiera się na danych osobowych, a więc podlega przepisom z tego zakresu. Od 25 maja 2018 r. w całej Unii Europejskiej stosuje się Rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylenia Dyrektywy 95/56/WE (Ogólne Rozporządzenie o ochronie danych, RODO).

Głównym celem pracy jest analiza uprawnień osób profilowanych oraz skuteczności ochrony jednostki przed wspomnianymi powyżej zagrożeniami wynikającymi z profilowania.

Profilowanie może nieść ze sobą mniej lub bardziej znaczący dla jednostki efekt, negatywny bądź pozytywny, korzystny lub niekorzystny, sprawiedliwy lub niesprawiedliwy, słuszny lub niesłuszny, poprawny bądź błędny, zgodny z prawem bądź bezprawny. Np. odmowa kredytu w wyniku działania algorytmu profilującego jest dla osoby niekorzystna choć może być sprawiedliwa i poprawna. Ale poprawność należy odnieść do tego czy bank miał poprawne i wyczerpujące dane. Istnieje zatem potrzeba kontroli całego procesu podejmowania decyzji przez algorytm.

W pracy odnoszę się do trzech zasadniczych zagadnień:

- czy stosowane od 25 maja 2018 r. przepisy o ochronie danych stanowią skuteczną ochronę praw jednostki przed negatywnymi skutkami profilowania osób,
- w jakim kierunku powinna ewoluować administracyjnoprawna regulacja związana z profilowaniem i podejmowaniem na jego podstawie zautomatyzowanych decyzji, oraz
- jakie działania w ramach obecnego stanu prawnego należy podjąć, aby profilowanie było bezpieczniejsze i dokładniejsze.

### *4.3 Struktura pracy*

Praca składa się z sześciu rozdziałów. W rozdziale I opisano podstawowe zagadnienia związane z profilowaniem, w tym podstawy technik analitycznych używanych do profilowania.

Opisałem narzędzia typu *Big data* oraz podstawowe zasady działania algorytmów profilujących, wskazano także znaczenie użycia sztucznej inteligencji w omawianych procesach. Przytaczam także wiele przykładów praktycznych, w tym opisuję najważniejsze algorytmy profilujące w Internecie. Następnie przechodzę do analizy zagrożeń, jakie dla jednostek może nieść profilowanie. Głównymi zidentyfikowanymi zagrożeniami są, jak wspomniałem, naruszenia sfery prywatności, dyskryminacja i doprowadzenie do manipulowania ludźmi. Opisuję każde z tych zagrożeń, wskazując jednocześnie w jaki sposób profilowanie może do nich prowadzić (rozdział II). Z uwagi na to, że profilowanie ludzi wiąże się z wykorzystaniem danych osobowych, na problem ten zwrócił uwagę prawodawca unijny a za nim polski ustawodawca wprowadzając już ponad 20 lat temu do naszego prawa pojęcie zautomatyzowanych decyzji, czyli czynności podejmowanych wobec jednostek bez udziału człowieka. W Rozporządzeniu ogólnym o ochronie danych osobowych (RODO), zwrócono dodatkowo uwagę na samą czynność profilowania, która może poprzedzać zautomatyzowaną decyzję podejmowaną wobec jednostki. Prawodawca unijny zdaje sobie sprawę z zagrożeń, jakie mogą wynikać ze zautomatyzowanego przetwarzania danych. W RODO wskazuje się m. in. na to, że profilowanie i jego wyniki opierają się w znacznej mierze na metodach matematycznych i statystycznych, które nie są wolne od błędów.

Biorąc pod uwagę powyższe zagrożenia w rozdziale III podejmuję próbę oceny skuteczności rozwiązań przyjętych w RODO z perspektywy ochrony praw jednostki. Identyfikuję zatem cele tej regulacji prawnej, następnie przedstawiam ogólne warunki oceny skuteczności administracyjnoprawnej ochrony danych osobowych. W kolejnym rozdziale przeprowadzam szczegółową analizę przyjętych w RODO oraz towarzyszących mu aktach prawnych rozwiązań dotyczących zarówno profilowania jak i zautomatyzowanych decyzji będących jego wynikiem (rozdział IV).

Szczególną uwagę zwracam na obowiązki administratorów danych wobec jednostki w kontekście profilowania (rozdział V). Wykazuję m. in. że transparentność tego rodzaju przetwarzania danych wobec osoby profilowanej jest w RODO bardzo ograniczona. Jednostka może też nie mieć odpowiedniej wiedzy, aby zrozumieć sposób działania algorytmów profilujących, dlatego tak istotne znaczenie może mieć wsparcie ze strony wyspecjalizowanego organu, jakim w Polsce jest Prezes Urzędu Ochrony Danych Osobowych. W rozdziale VI analizuję uprawnienia organu w kontekście możliwości prawidłowej oceny procesów profilowania, następnie wskazuję na mankamenty i niejasności RODO w omawianym zakresie. Praca zawiera rekomendacje zarówno *de lege ferenda*, jak i wskazówki co do interpretacji

RODO, a także rekomendacje co do działań podjętych na jego podstawie, które miałyby prowadzić do polepszenia skuteczności ochrony praw jednostki.

### *4.4 Wnioski*

W pracy oceniam przede wszystkim skuteczność finitystyczną regulacji, a więc to czy ma ona szansę doprowadzić do realizacji celów postawionych przed RODO. Skuteczność przyjętych w RODO rozwiązań w zakresie ochrony praw jednostki w związku z profilowaniem i podejmowaniem w stosunku do niej zautomatyzowanych decyzji ma zatem służyć wzrostowi zaufania ludzi do cyfrowych usług. Pośrednie cele zostały wyrażone w RODO w postaci m. in. zasad ogólnych przetwarzania danych. Na tak rozumianą skuteczność składa się szereg elementów.

#### *a) Poprawność identyfikacji celu regulacji*

RODO wpisuje się w działania Unii Europejskiej związane z rozwojem usług opartych na nowych technologiach. Głównym celem tej regulacji jest bezpieczeństwo korzystania z sieci i e-usług oraz budowa zaufania użytkowników tych usług. Z tej perspektywy zaufanie musi opierać się przede wszystkim na następujących elementach:

- legalność procesów przetwarzania danych w tym profilowania,
- transparentność tych procesów,
- bezpieczeństwo danych oraz
- administracyjnoprawne instrumenty wspomagające podmiot danych.

Warunkiem poprawnej identyfikacji celu jest również prawidłowe zdefiniowanie zagrożeń. W odniesieniu do profilowania w RODO wskazano szereg zagrożeń, co oznacza, że prawodawca miał świadomość ryzyka, jakie profilowanie i oparte na nim zautomatyzowane decyzje mogą nieść dla jednostki.

#### *b) Zakres regulacji*

Prawodawca unijny zdawał sobie sprawę ze stale rozszerzającego się zasięgu przetwarzania danych osobowych, w tym profilowania, dlatego RODO dotyczy nie tylko podmiotów przetwarzających danych na terenie UE, ale również tych, które przetwarzają dane w związku z oferowaniem na terenie UE towarów i usług lub monitorowaniem osób przebywających w Unii, a niemających siedziby w UE. Rozwiązanie to należy ocenić pozytywnie, chociaż praktyka pokaże dopiero jego skuteczność. Będzie ona w dużej mierze zależała od

egzekwowalności administracyjnych kar pieniężnych nakładanych na podmioty spoza UE (jak w omawianej w pracy decyzji CNIL w sprawie kary nałożonej na Google).

*c) Dobór instrumentu prawnego*

RODO jako unijne rozporządzenie znajduje bezpośrednie zastosowanie bez potrzeby implementacji w prawie krajowym. RODO zastępując Dyrektywę 95/46 miało doprowadzić do ujednolicenia stosowania reguł ochrony danych osobowych. Implementacja Dyrektywy 95/46 spowodowała zbyt wiele różnic w regulacji tej ochrony. Jednolite stosowanie RODO jest jednak wątpliwe, m. in. ze względu na możliwość ograniczenia w ustawodawstwie krajowym praw podmiotów danych (na podstawie art. 23 RODO).

*d) Język aktu prawnego*

Jeśli przyjąć, że akt prawny powinien być napisany w taki sposób, żeby był zrozumiały dla przeciętnego obywatela, to RODO takiego wymogu nie spełnia. Nie chodzi jedynie o to, że pewne sformułowania mają różne znaczenie w różnych systemach prawnych, ale także o sprzeczności wewnętrzne, nieprecyzyjne sformułowania w przepisach, których nieprzestrzeganie grozi konsekwencjami, w tym wysokimi karami pieniężnymi.

e) ***Kompletność rozwiązań, środków i instrumentów prawnej kontroli procesów przetwarzania.***

W mojej ocenie RODO w kontekście profilowania i zautomatyzowanych decyzji daje podmiotom ułomne instrumenty kontroli nad tymi czynnościami. W świetle zagrożeń, jakie mogą wynikać z tych operacji, zakres uprawnień, w tym transparentność profilowania dla podmiotu danych jest ograniczona. Nie ma obowiązku informowania o samym fakcie profilowania, a podjęcie zautomatyzowanej decyzji nie powoduje konieczności wyjaśnienia powodów jej podjęcia. Adresat decyzji może uprzednio poznać jedynie zasady podejmowania decyzji i konsekwencje, ale jest to informacja ex ante w przypadku obowiązku informacyjnego (art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g) RODO), a w przypadku skorzystania z prawa dostępu (art. 15 ust. 1 lit. h) RODO) administrator nie ma obowiązku podania szczegółów konkretnej zautomatyzowanej decyzji.

Pojawia się również pytanie czy osoba, która nie jest adresatem konkretnej decyzji (np. sędzia, który nie został przez algorytm wybrany do składu orzekającego w sądzie) może skorzystać z uprawnień przewidzianych w art. 22 ust. 3 RODO, tj. prawa do uzyskania interwencji ludzkiej

ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Przepis ten jako legitymowaną wskazuje osobę, której dane dotyczą.

Brak całkowitej transparentności to nie jedyne ograniczenie dla podmiotu danych. Jednostka nie ma faktycznej kontroli nad bezpieczeństwem profilowania i jego poprawnością, ewentualne zgłoszenie problemu lub wątpliwości może dotyczyć bowiem sytuacji, w której ma podejrzenie naruszenia. RODO nie zawiera mechanizmu uprzedniej kontroli poprawności algorytmów i metod tworzenia modeli predykcyjnych.

***f) Rodzaj wsparcia jakie jednostka otrzymuje ze strony państwa.***

W związku z ograniczeniem wobec podmiotu danych transparentności profilowania i kontroli nad zautomatyzowanymi decyzjami, szczególnego znaczenia nabierają kompetencje organu nadzorczego. Mam tu na myśli uprawnienia kontrolne i instrumenty wpływu na poprawność profilowania oraz na prawidłowość dokonanej przez administratora oceny skutków przetwarzania. Wydaje się, że organ nadzorczy dysponuje odpowiednim zakresem uprawnień do kontroli poprawności profilowania. Odrębną kwestią są środki finansowe i kwalifikacje pracowników organu. Zważywszy, że kontrola algorytmów profilujących i modeli predykcyjnych będzie wymagała w większości przypadków bardzo specjalistycznej wiedzy, potrzebne będzie sięgnięcie do ekspertów zewnętrznych. To z kolei będzie generować wyższe koszty rozpatrywania skarg podmiotów danych.

***g) Skuteczność, w tym egzekwowalność działań organu.***

Niewątpliwie skuteczność przestrzegania RODO będzie zależała od podejścia administratorów, podmiotów przetwarzających oraz działań organów nadzorczych, w tym w zakresie nakładania administracyjnych kar pieniężnych. Wydaje się, że wysokość kar oraz kryteria ich stosowania (skuteczne, proporcjonalne i odstraszające) może pozytywnie wpłynąć nie tylko na przestrzeganie RODO, ale również na działania administratorów i podmiotów przetwarzających danych na zlecenie administratorów, aby chronili oni dane osobowe w stopniu większym niż przewidziany w RODO.

***h) Rola aktów wykonawczych i delegowanych***

Komisja Europejska może m. in. przyjąć akty wykonawcze określające techniczne standardy mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposoby upowszechniania i uznawania tych mechanizmów certyfikacji oraz znaków

jakości i oznaczeń (art. 43 ust. 9 RODO), oraz akty delegowane w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych (art. 12 ust. 8 RODO), a także akty delegowane w celu doprecyzowania wymogów, które uwzględnia się w przypadku mechanizmu certyfikacji (art. 43 ust. 8 RODO). Akty te mogą zwiększyć transparentność profilowania i podnieść poziom poprawności tych operacji.

*i) Wypowiedzi właściwych organów: opinie i wytyczne właściwych organów*

RODO przewiduje możliwość wydawania przez organy opinii i wytycznych dotyczących stosowania jego przepisów. Nie mają mocy wiążącej, ale ich rolą jest pomoc w interpretacji i stosowaniu przepisów unijnych. Ich skuteczność może być dzięki temu większa.

*j) Edukacja*

Praktyka wdrożenia RODO w firmach i instytucjach wskazuje, że zarówno świadomość profilowania jak i zrozumienie jego istoty jest niezwykle trudne. Stąd ważna jest edukacja zarówno społeczeństwa, jak i organów stosujących prawo w zakresie przede wszystkim konsekwencji profilowania i sytuacji, w których możemy się z nim spotkać.

W pracy zawarłem szereg **rekomendacji**.

Punktem wyjścia do ich sformułowania, jest stwierdzenie, że w obecnych warunkach w profilowaniu nadal mamy do czynienia ze statystyką, być może coraz dokładniejszą, ale jednak niosącą ryzyko błędów, które mogą mieć dla obywateli i konsumentów ogromne znaczenie.

Prawodawca unijny tworząc RODO niewątpliwie zdawał sobie sprawę z zagrożeń wynikających z profilowania, większość z nich wyartykułował w preambule bądź w konkretnych przepisach. Zabrakło jednak spójnego podejścia do tego typu przetwarzania i jego konsekwencji. Można się zgodzić z argumentem, że transparentność profilowania powinna mieć swoje granice: niewątpliwie jest nią konieczność zachowania algorytmów i modeli predykcyjnych w poufności w warunkach gry rynkowej, ponieważ informacje te często decydują o przewadze konkurencyjnej (mogą też decydować np. o powodzeniu w wyborach). Drugim czynnikiem ograniczającym jest niewątpliwie skomplikowanie materii, o której mowa, które każe wątpić w możliwość zrozumienia wszystkich mechanizmów działania algorytmów i modeli przez przeciętnego konsumenta. Konsument powinien znać ogólny mechanizm działania, nie powinniśmy natomiast moim zdaniem dążyć do poznania przez konsumenta

szczegółów działania algorytmów w sektorach mających istotne znaczenie dla bezpieczeństwa i porządku publicznego oraz ważnego interesu gospodarczego. To z kolei każe w mojej ocenie wzmocnić rolę organów publicznych (organów państwa i instytucji unijnych), ponieważ to do nich powinno należeć badanie szczegółów omawianych czynności.

Z powyższych względów duże znaczenie ma określenie warunków profilowania co najmniej w przypadku profilowania pośredniego na dużych zbiorach danych, poprzedzonego budowaniem modelu predykcyjnego poprzez m. in. rekomendację przeprowadzania testów modeli na wydzielonych zbiorach danych.

Należałoby moim zdaniem rozstrzygnąć, że z uprawnień przewidzianych w art. 22 ust. 3 RODO (tj. prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji) może skorzystać również osoba, która nie jest adresatem zautomatyzowanej decyzji, ale jej dane osobowe są przedmiotem przetwarzania w procesie poprzedzającym decyzję.

Należy także rozważyć wprowadzenie szczególnego mechanizmu certyfikacji dla omawianych procesów i włączenie w ten mechanizm wyspecjalizowanych instytucji naukowych i innych, które mogłyby służyć wiedzą na temat używanych algorytmów i budowy modeli predykcyjnych.

Odrębną kwestią jest doprowadzenie do obowiązku wykonywania oceny skutków przetwarzania dla wszystkich operacji profilowania, niezależnie od tego czy ich wynikiem jest zautomatyzowana decyzja.

Odnośnie do zarzutu ograniczenia transparentności, zasadny wydaje się postulat zmiany RODO poprzez dodanie do uprawnień osoby profilowanej obowiązku wyjaśnienia każdej decyzji. Wyjaśnialność powinna być ograniczona do obowiązku podania najważniejszych czynników, które wpłynęły na treść decyzji. Komisja Europejska powinna w akcie delegowanym wprowadzić obowiązek ostrzegania o profilowaniu i podejmowaniu zautomatyzowanych decyzji za pomocą znaków graficznych (ikonek).

Zgadzam się także z postulatem, aby rozważyć powołanie organu lub organów ds. profilowania (ang. profiling authority). Jednym z powodów tej propozycji jest przewidywana niska skuteczność indywidualnych skarg w połączeniu z brakiem całkowitej transparentności procesów przetwarzania. Organ taki miałby być wyposażony w uprawnienia do aktywnej kontroli (ang. active investigation) procesów profilowania. Alternatywą dla powołania

odrębnego organu kontrolującego procesy profilowania może być większa współpraca organów ochrony danych i organów właściwych ds. ochrony konsumenta, radiofonii i telewizji oraz organów odpowiedzialnych za przeprowadzanie wyborów. We wszystkich wymienionych dziedzinach mamy do czynienia z nadużyciami wynikającymi z profilowania.

## 5. Omówienie pozostałych osiągnięć naukowo - badawczych.

### *5.1 Uwagi ogólne*

Po otrzymaniu tytułu doktora nauk prawnych moje zainteresowania koncentrowały się głównie wokół prawnej ochrony sfery prywatności i danych osobowych.

Zajmowałem się również prawnymi aspektami cyberbezpieczeństwa, dostępem do informacji publicznej oraz innymi zagadnieniami z zakresu prawa administracyjnego, w tym regulacjami wybranych rynków (telekomunikacyjnego i lotniczego). Zajmowałem się również współpracą administracji i sektora prywatnego przy wykonywaniu zadań publicznych, a także etyką zawodów prawniczych.

W tym okresie zorganizowałem na Wydziale Prawa i Administracji UW sześć konferencji naukowych: pięć poświęconych ochronie danych osobowych (współorganizowanych przez Dziekana WPiA i Generalnego Inspektora Ochrony Danych Osobowych) oraz konferencję poświęconą rynkowi lotniczemu (z udziałem prezesa firmy Ryanair, p. Michaela O'Leary). Ta ostatnia została zorganizowana wspólnie z Wydziałem Zarządzania UW. Ponadto, uczestniczyłem w wielu konferencjach naukowych poświęconych ochronie danych osobowych w kraju i za granicą.

Po otrzymaniu tytułu doktora opublikowałem ponad 60 pozycji naukowych, których byłem autorem, współautorem lub redaktorem. Wśród publikacji znalazło się 10 książek, w tym dwutomowa publikacja „Misja publiczna, Wspólnota, państwo. Studia z prawa i administracji. Księga dedykowana pamięci Profesora Michała Kuleszy" (Warszawa 2016).

Pełna lista moich publikacji naukowych wydanych po otrzymaniu tytułu doktora nauk prawnych znajduje się w załączniku nr 5.

### *5.2 Prawo do prywatności, ochrona danych osobowych, cyberbezpieczeństwo.*

Ponad 30 ze wspomnianych powyżej publikacji było poświęconych teoretycznym i praktycznym aspektom prawa ochrony danych, w tym poszczególnym uprawnieniom podmiotu danych oraz obowiązkom administratorów danych. Zajmowałem się również tajemnicami zawodowymi i sektorowymi i relacją tych tajemnic do przepisów o ochronie danych osobowych.

W 2018 r. byłem współautorem podręcznika pt. Cyberbezpieczeństwo (red. C. Banasiński). Tematyka ta ma wiele wspólnego z ochroną danych, choć obie dotyczą bezpieczeństwa informacji widzianego z różnych perspektyw (przepisy o cyberbezpieczeństwie mają na celu zachowanie ciągłości usług określanych jako kluczowe, oraz niektórych usług cyfrowych, a prawo ochrony danych – dotyczy praw i wolności osób fizycznych).

### *5.3 Dostęp do informacji publicznej*

Drugim ważnym obszarem moich zainteresowań naukowych i praktycznych jest jawność życia publicznego, w tym dostęp do informacji publicznej. Opublikowałem wybór orzecznictwa dotyczącego relacji pomiędzy jawnością a prywatnością oraz dwa artykuły dotyczące dostępu do informacji publicznej. Prowadzę również wykłady poświęcone dostępowi do informacji publicznej.

### *5.4 Rynki regulowane*

Przedmiotem moich zainteresowań są również regulacje wybranych rynków, w szczególności telekomunikacyjnego i lotniczego.

W 2015 r. zorganizowałem na WPiA UW konferencję poświęconą regulacjom rynku lotniczego, a kilkanaście publikacji poświęciłem różnym zagadnieniom z zakresu prawa telekomunikacyjnego. Dotyczyły one m. in. inwestycji w telekomunikacji, stawek międzyoperatorskich, usługi powszechnej, itp. Prowadzę także zajęcia z europejskiego i polskiego prawa łączności elektronicznej.

### *5.5 Administracja publiczna, w tym formy realizacji zadań publicznych*

W ramach działalności naukowej zajmowałem się również samorządem terytorialnym oraz formami wykonywania zadań publicznych, w tym w szczególności partnerstwem publiczno-prywatnym i koncesją na roboty budowane i usługi.

### *5.6 Parametryzacja osiągnięć naukowych*

Według Google Scholar (https://scholar.google.pl/citations?hl=pl&user=FMfg6vIAAAAJ) ogólna liczba cytowań moich publikacji wynosi 124, h-indeks wynosi 6, a indeks i10 – indeks wynosi 5.

### *5.7 Międzynarodowe i krajowe konferencje naukowe*

Wykaz krajowych i międzynarodowych konferencji, na których (po uzyskaniu stopnia doktora) wygłaszałem prelekcje znajduje się w załączniku nr 6 do wniosku habilitacyjnego

## 6. Dorobek dydaktyczny i działalność na Uniwersytecie Warszawskiem

Szczegółowa informacja na temat mojej działalności dydaktycznej, promocji prac magisterskich i dyplomowych, a także innej działalności na rzecz Uniwersytetu Warszawskiego znajduje się w załączniku nr 7 do wniosku habilitacyjnego.

## 7. Działalność ekspercka i zawodowa

W latach 2008-2009 w Nadzwyczajnej Komisji Sejmowej Przyjazne Państwo byłem ekspertem ds. prawa administracyjnego z ramienia Okręgowej Izby Radców Prawnych w Warszawie.

W roku 2013 brałem udział w projekcie badawczym „Wykorzystanie danych z rejestrów publicznych budowanych w ramach 7 Osi POIG". Organizatorem była Władza Wdrażająca Programy Europejskie w ramach Projektu Systemowego dla wspierania działań w zakresie budowy elektronicznej administracji Program Operacyjny Innowacyjna Gospodarka 7. Oś Priorytetowa.

Jestem członkiem Rady programowa czasopisma Informacja w administracji publicznej, wyd. C.H. Beck.

W latach 2013 – 2015 byłem członkiem Rady Naukowej przy Generalnym Inspektorze Ochrony Danych Osobowych (dokładna data zakończenia działalności Rady nie jest znana).

Jestem radcą prawnym zrzeszonym w OIRP Warszawa. Do września 2017 byłem wspólnikiem w kancelarii Wierzbowski Eversheds Sutherland. Od października 2017 r prowadzę praktykę TMT/IP&Data protection w PwC Legal.

W ostatnich latach byłem wielokrotnie nagradzany w rankingach Chambers (m. in. I miejsce w 2019 r.), Legal500, Polityki Insight, Rzeczpospolitej w kategoriach Ochrona danych osobowych oraz Telekomunikacja Media Technologie.