Prof. dr hab. Dagmara Kornobis-Romanowska
Katedra Badań nad Prawem Europejskim im. Jeana Monneta
Centrum Doskonałości im. Jeana Monneta
Katedra Prawa Międzynarodowego i Europejskiego
Uniwersytet Wrocławski

Wrocław, dnia 5 września 2021 r.

Recenzja rozprawy doktorskiej
mgr Aleksandry Kacały-Szwarczyńskiej
na temat:
Profilowanie w Internecie w celu przeciwdziałania terroryzmowi
Studium z zakresu prawa europejskiego
(Promotor: Dr hab. Joanna Nowakowska-Małusecka, prof. UŚ,
Katowice 2021)

1. Wybór tematu rozprawy

Problem prawny rozprawy dotyczy szczególnych metod i mechanizmów wypracowanych przez społeczność międzynarodową w celu zapobiegania, wykrywania i zwalczania przestępczości międzynarodowej w formie działalności terrorystycznej. W przedmiotowej rozprawie są to metody i mechanizmy uruchamiane za pomocą nowoczesnych technologii informatycznych pozwalających na śledzenie aktywności i komunikacji transgranicznej mające służyć zapobieganiu rozpowszechnianiu treści terrorystycznych, uniemożliwieniu radykalizacji, rekrutowania ludzi do popełniania aktów terroryzmu, propagowania przemocy, organizowania przeprowadzania zamachów terrorystycznych. Korzystanie z narzędzi cyfrowych w całej Europie, jak i na

świecie, ma kluczowe znaczenie dla skutecznego zapobiegania zamachom terrorystycznym. Jednym z nich jest tytułowe dla recenzowanej dysertacji profilowanie w sieci, które polega na automatycznym gromadzeniu przez organy ścigania danych o sprawcach w celu kategoryzacji osób i przetwarzania tych informacji w celu zbudowania pewnych założeń i modeli zachowań, by ostatecznie na tej podstawie ocenić te zachowania, sytuację i inne aspekty osobiste osób fizycznych podejrzewanych o terroryzm. Ocena ta jest zatem nową informacją, wywiedzioną w drodze wykorzystania techniki automatycznej. Takie rozumienie pojęcia profilowania przyjęte jest w UE, co wyraża m.in. definicja legalna zawarta w art. 4 pkt 3a RODO, a także w ramach Rady Europy. Jej zastosowanie niechybnie prowadzi do ingerencji w prywatność i autonomię informacyjną, może prowadzić do dyskryminacji, wykluczenia, głownie z powodu narodowości, i segregacji społecznej. W konsekwencji naruszone mogą być wartości, które wiążą się z praworządnością, prawami i wolnościami człowieka, chronione przez akty prawne najwyższej ragi we wszystkich systemach prawa – tak na szczeblu międzynarodowym, unijnym, jak i krajowym. Ogólne rozwiązania prawne, takie jak konwencje Rady Europy, akty przyjmowane przez instytucje unijne (tak jak np. RODO), czy ustawodawstwo krajowe, zawierające generalny zakaz podejmowania ostatecznych rozstrzygnięć w sprawie indywidualnej na podstawie danych osobowych, jeżeli treść takiego rozstrzygnięcia jest wyłącznie wynikiem operacji na tych danych, prowadzonych w systemie informatycznym, nie są w stanie zapewnić w pełni poszanowania praw i wolności obywatelskich, stąd potrzeba przyjmowania szczegółowych regulacji prawnych, nadzoru jurysdykcyjnego, gwarancji proceduralnych oraz monitorowania praktyk z zakresu profilowania. Celem jest budowa systemu opartego na współpracy podmiotów międzynarodowych służącego zapobieganiu radykalizacji i ochronie wartości, przy jednoczesnym zapewnieniu bezpieczeństwa obywatelom w Europie.

Biorąc powyższe ustalenia pod rozwagę, należy uznać wybór tematu pracy za trafny, ambitny i o dużym znaczeniu nie tylko teoretycznoprawnym, ale i praktycznym. Problem prawny pracy jest z zakresu prawa międzynarodowego o zasięgu kontynentalnym, ilustrowany rozwiązaniami przyjętymi na poziomie krajowym przez wybrane państwa (Belgia, Francja, Niemcy, Polska i Wielka Brytania). Badania dotyczą zatem prawa europejskiego, w tym zarówno prawa Unii UE, jak i prawa tworzonego i obowiązującego w ramach Rady Europy (RE) dotyczącego praw człowieka, w tym

głównie ochrony danych osobowych, prawa do prywatności w konfrontacji z zasadami bezpieczeństwa państwa. Zgodnie ze wskazaniem Autorki na s. 8, tak obrany zakres badań podyktowany był wprowadzeniem w Europie najbardziej zaawansowanych na świecie **standardów** z zakresu ochrony danych osobowych. Termin „standard" w tym kontekście należy uznać za wyjątkowo trafny i stanowiący sedno problemu prawnego dla recenzowanej dysertacji. Już w pierwszym akapicie Wstępu (s. 7) Autorka zauważa, że „W praktyce okazało się jednak, że normy z zakresu bezpieczeństwa trudno pogodzić z wysokim standardem ochrony praw człowieka wprowadzonym w reformie ochrony danych osobowych". Rozwijając konsekwentnie ten wątek, Autorka wskazuje główne zadanie badawcze (s.8-9), jakim jest weryfikacja tezy, że obowiązujące rozwiązania prawne nie zapewniają **skutecznej** ochrony osób, których dane dotyczą, w związku ze stosowaniem przez państwa narzędzi masowej inwigilacji,takich jak profilowanie, w celu zapewnienia bezpieczeństwa. Już na Wstępie Autorka rozpoznaje największe deficyty w tym przedmiocie, tj. brak jasnych definicji i korzystanie z pojęć abstrakcyjnych w odniesieniu do poważnej przestępczości z wykorzystaniem technologii doprowadzają do powstania ryzyka nadużycia prawa w stosunku do jednostek, oraz brak przepisów prawa w zakresie rozwoju narzędzi technologicznych, takich jaksztuczna inteligencja, *big data,* chmury obliczeniowe, uczenie maszynowe, które używane są w trakcie profilowania, rozwijane jest tzw. miękkie prawo (normy etyczne, kodeksy postępowania i checklisty audytowe). Jak dalej zauważa Doktorantka, także standardy wyznaczane przez UE w zakresie ochrony danych osobowych nie zabezpieczają dostatecznie praw osób poza granicami Unii, co wobec transgranicznego charakteru działania Internetu, co jest niezbędne, by ochrona praw tych osób była skuteczna.

Jak zatem wynika z tytułu oraz ze Wstępu, pierwszoplanowe założenie badawcze stanowią **standardy** ochrony danych osobowych, które są przyjęte w Europie w celu przeciwdziałania terroryzmowi z wykorzystaniem techniki informatycznej, jaką jest profilowanie. Zakres badań obejmuje zatem przedstawienie tych standardów wraz z oceną ich skuteczności na poziomie międzynarodowym oraz w wybranych państwach europejskich.

Kierując się powyższymi założeniami badawczymi, należy uznać, że przedmiotową tezę zawartą w tytule recenzowanej rozprawy można także wyrazić alternatywnie, w następujący sposób:

Europejskie standardy dotyczące profilowania w Internecie w celu przeciwdziałania terroryzmowi, ramy wykonania i skuteczność.

Wydaje się, że takie brzmienie tytułu precyzyjniej i w sposób bardziej uporządkowany oddawałoby temat dysertacji, a także jej treść, o czym szerzej w dalszej części tej recenzji dotyczącej oceny merytorycznej. Sam problem badawczy przy tak zmodyfikowanym brzmieniu tytułu pozostaje jednak bez zmian, jest to więc kwestia głównie redakcyjna.

Uwzględniając powyżej wskazane zastrzeżenia odnośnie do brzmienia tytułu, wybór tematu rozprawy należy ocenić jednoznacznie pozytywnie. Nie budzi wątpliwości, że problematyka objęta tym tematem ma olbrzymią doniosłość prawną, tak w teorii, jak i w praktyce. Pole badań zakreślone w tytule i dookreślone we Wstępie do rozprawy należy więc uznać za trafne, ambitne i zasługujące na pozytywną ocenę.

2. Konstrukcja i systematyka pracy - uwagi ogólne

Recenzowana rozprawa doktorska liczy ogółem 270 stron, na które składa się spis treści, Wstęp, pięć rozdziałów, Zakończenie i bibliografia.

Przedmiotem rozdziału I są „zagadnienia wprowadzające", przez które Doktorantka rozumie takie kwestie, jak historia Internetu i rozwój społeczeństwa informacyjnego, pojęcia profilowania i terroryzmu oraz ich ramy prawne w przestrzeni międzynarodowej, w tym w systemie ONZ, RE i UE. Należy żałować, że rozdział ten jest niejako przybudówką, a nie integralną częścią pracy, o czym wyraźnie świadczy sam jego tytuł, w którym nie został zawarty żaden konkretny problem prawny. Dodatkowo w systematyce tego rozdziału kwestie ewolucji podejścia do profilowania na arenie międzynarodowej zostały przedstawione z perspektywy powszechnego prawa międzynarodowego (ONZ), w uzupełnieniu przez prawo europejskie. Takie podejście stanowi jednak uogólnienie niż konkretyzację tematu i z pewnością normy europejskie powinny być na pierwszym planie.

Rozdział II recenzowanej dysertacji nosi tytuł „Profilowanie z wykorzystaniem systemów informatycznych" i zawiera takie zagadnienia szczegółowe, jak zakres i zasady profilowania, rodzaje przetwarzanych danych osobowych oraz podmioty uprawnione do profilowania. Jest to zatem zakres podmiotowy i przedmiotowy profilowania, uzupełniony przez charakterystykę tej techniki informatycznej w postaci automatyzacji podejmowania decyzji oraz kwestię dopuszczalności przekazywania danych do państw trzecich i do organizacji międzynarodowych, co ma olbrzymie znaczenie dla przeciwdziałania międzynarodowemu terroryzmowi. Podobnie jak w przypadku uwag sformułowanych odnośnie do rozdziału I, także i w tej części pracy akcenty rozłożone są nierówno i niejasno. Sam tytuł nie doprecyzowuje zakresu prowadzonych badań, nie wynika to także z podtytułów. Punkt 1 to ścisłe prawo unijne („Zakres profilowania w Dyrektywie Policyjnej"), natomiast kolejne punkty w tym rozdziale to normy i zasady z różnych systemów potraktowane zbiorczo, bez próby ich kategoryzacji i usystematyzowania na poziomie konstrukcji pracy. Należy zauważyć, że w treści pracy, ocenianej w kolejnym punkcie tej recenzji, ta systematyka ma miejsce. Nie jest jednak uwidoczniona w planie ogólnym.

Kolejny, III rozdział dotyczy gwarancji ochrony praw człowieka w procesie profilowania. Doktorantka wstępnie analizuje warunki dopuszczalności derogacji praw człowieka przewidziane prawem międzynarodowym, w tym związane z zagrożeniem terrorystycznym. Dalej, w punkcie 3, Doktorantka przechodzi bezpośrednio na grunt prawa unijnego, a konkretnie do dyrektywy policyjnej (DODO) i do przyznanych na jej podstawie uprawnień przysługujących jednostkom w przypadku profilowania (prawo dostępu do danych, do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania). W ramach tego punktu wskazane są także obowiązki dokumentacyjne administratorów danych. Biorąc pod uwagę treść tego punktu, jego tytuł brzmiący „Mechanizmy ochronne (...)" jest nietrafiony. Punkt ten nie dotyczy bowiem zagadnień proceduralnych tylko materialnoprawnych. Wreszcie ostatni, 4 punkt w tym rozdziale nosi tytuł „Organ nadzoru nad bezpieczeństwem danych" – w liczbie pojedynczej, podczas gdy treść dotyczy obowiązków i zasad działania inspektorów nadzoru danych oraz państwowych organów nadzoru. Wszystko to sprawia, że systematyka tego rozdziału, a w szczególności punktów 3 i 4 jest problematyczna i niejasna. Począwszy więc od tytułu tego rozdziału po śródtytuły

należałoby doprecyzować o jakie gwarancje chodzi – materialnoprawne, proceduralne, instytucjonalne, wymaga to jednak także przegrupowania treści w ramach poszczególnych punktów i podpunktów.

Czwarty rozdział pracy traktuje o „ryzykach związanych z profilowaniem", wliczając w to błędy i brak transparentności, dyskryminację, naruszenie prawa do prywatności oraz prawa dobycia zapomnianym. Tytułowe dla tego rozdziału „ryzyko" sugeruje, że organy ścigania świadomie i celowo podejmują czynności związane z prawdopodobieństwem naruszenia prawa i powstania szkody po stronie jednostek. Jeśli jednak działania te nie są celowe, wówczas obok ryzyka można mówić o zagrożeniach. Warto je więc uwzględnić w zakresie przedmiotowego rozdziału.

Wreszcie ostatni, piąty rozdział poświęcony jest, zgodnie z tytułem, praktycznym aspektom profilowania oraz programom masowej inwigilacji. Punktem wyjścia do tych badań jest przedstawienie, jak programy masowej inwigilacji mogą być wykorzystywane w walce z terroryzmem, w szczególności w działaniach UE i RE. Kolejny etap badań, to praktyka na tym polu przyjęta przez wybrane państwa europejskie tj. Belgia, Francja, Niemcy, Polska i Wielka Brytania.

Każdy z rozdziałów pracy doktorskiej wieńczy Podsumowanie.

Ostatecznie oceniając konstrukcję i systematykę pracy należy uznać, że są one w zasadzie prawidłowe. Praca pod tym względem jest uporządkowana, choć wątpliwości mogą budzić niektóre tytuły i podtytuły, które w niektórych przypadkach są sformułowane w sposób bardzo ogólnikowy (jak rozdział I: „Zagadnienia wprowadzające"), niedoprecyzowany ze względu na zakres normowania, bądź treść. Należy także zauważyć, że rozwiązania prawne w UE i RE nie zawsze są pierwszoplanowe i bywa, że ustępują pola normom przyjętym w powszechnym systemie prawa międzynarodowego (ONZ). Tymczasem, biorąc pod uwagę tytuł pracy, jak i wyjaśnienia zawarte we wstępie, te ostatnie mają dla pracy stanowić jedynie dopełnienie, bądź tło, jak Doktorantka zapowiada na stronie 8 recenzowanej dysertacji. Takie ujęcie sprawia, że zestawienie przedmiotowych problemów nie zawsze jest logiczne i spójne. Są to jednak wady, które nie mają jednak decydującego wpływu na ostateczną ocenę ogólną tej warstwy opracowania. Ocena ta jest pozytywna.

3. Ocena merytoryczna pracy

Problem badawczy w przedstawionej pracy jest z zakresu prawa międzynarodowego i unijnego. Punktem stycznym dla obu zakresów jest krajowe wykonanie w prawie krajowym wybranych państw europejskich, tj. Belgia, Francja, Niemcy, Polska i Wielka Brytania. Wszystkie te państwa są członkami RE, a do UE nie należy (już) Zjednoczone Królestwo, które od 1.02.2020 jest dla UE państwem trzecim. Niestety, na stronach recenzowanej rozprawy fakt ten nie został odnotowany, nie ma też mowy o następstwach brexitu dla zobowiązań brytyjskich w przedmiotowej materii. Na str. 125 Doktorantka wskazuje np., że „Parlament Europejski wezwał wszystkie państwa członkowskieUE, a w szczególności Wielką Brytanię (...)", a podobnie na str. 199 i n. W punkcie poświęconym w całości Zjednoczonemu Królestwu, stosowaniu dyrektyw, obowiązku zgodności prawa krajowego z prawem UE. Konkluzja do tego wątku brzmi, że „mimo prób formułowania prawa obejmującego masową inwigilację, UE nie wyraża zgody na funkcjonowanie takich mechanizmów. Widoczna jest spójność najnowszego orzecznictwa Unii z podstawowymi zasadami ochrony danych osobowych, a w szczególności z zasadą minimalizacji danych". Od razu rodzi się pytanie o zmiany powstałe w tym zakresie dla tego państwa w związku z brexitem, konsekwencje te nie zostały jednak uwzględnione na kartach recenzowanej rozprawy.

Znacząca część dysertacji została natomiast poświęcona kwestiom o charakterze historycznym i informacyjnym, niekoniecznie związanym z prawem europejskim, dotyczą natomiast zagadnień technologicznych o zasięgu globalnym. Informacje te są niewątpliwie ciekawe, bo dzięki nim można sobie przypomnieć, jak wyglądał świat bez Internetu i że Polska została podłączona do międzysieci dopiero w 1991 r. Autorka skrupulatnie wyjaśnia także znaczenie pojęć związanych z tematem, ale nie bezpośrednio, tj. informacja (s.17); społeczeństwo informacyjne (s. 16 i n.); system kryptowalut (s. 54); akcje ONZ dla zapobiegania terroryzmowi (s. 61-68); klauzule derogacyjne w powszechnym systemie praw człowieka (s. 132-137). Wydaje się, że bez szkody, a wręcz z korzyścią dla warstwy naukowej opracowania, można je było ograniczyć, a już na pewno ukierunkować ściśle na związek z profilowaniem. W innym wypadku podejmowanie tak uogólnionych wątków sprawia wrażenie, że dzieje się tak

niejako „przy okazji" i z pewnością w zakresie zbędnym dla głównego problemu badawczego.

Za nie dość jasne należy uznać za to wywody Doktorantki na temat dyrektywy policyjnej i zakresu jej stosowania w sprawach związanych z zagrożeniem terrorystycznym. Jak słusznie zostało ustalone na podstawie tego aktu normatywnego oraz z odwołaniem do literatury naukowej (głównie autorstwa prof. A. Grzelak), z motywu 14 tej dyrektywy wynika możliwość wyłączenia jej stosowania w razie przetwarzania danych w przeciwdziałaniu terroryzmowi jako zagrożeniu bezpieczeństwa narodowego. W konsekwencji, państwa członkowskie mają w tych przypadkach swobodę wyjścia poza wskazane ograniczenie i mogą poddać całościowej regulacji wszystkie sytuacje związane z przetwarzaniem danych osobowych do celów określonych w art. 1 dyrektywy policyjnej lub zrezygnować z jej stosowania w tym zakresie (s. 81). Jest to więc przykład wyłączenia przedmiotowego pozwalającego na niestosowanie dyrektywy do spraw wchodzących w zakres bezpieczeństwa narodowego, co zostało prawidłowo ustalone i skonstatowane przez Doktorantkę. Ustalenia te stanowią jednak przesłankę do wyprowadzenia ogólnego wniosku, że: „profilowanie, które zmierza do zapobieżenia aktowi terroryzmu lub wykrycia terrorysty, może nie być objęte przepisami Dyrektywy Policyjnej. Innymi słowy, gwarancje ochrony praw człowieka w tym zakresie mogą zostać istotnie ograniczone" (s. 82). Ale już kolejne zdanie w recenzowanej rozprawie brzmi: „Dyrektywa Policyjna zawiera ogólne zasady przetwarzania danych osobowych, które, jak wskazano zasadniczo powinny odnosić się do działalności służb delegowanych do walki z terroryzmem".

Należy podkreślić, że o ile powyższe konstatacje są trafne, logiczne i polegają na prawdzie, to brakuje jednak ich rozwinięcia, argumentacji i przede wszystkim uzasadnienia, szczególnie że dyrektywa policyjna stanowi w tej pracy główną podstawę prawną dla badań z zakresu prawa UE i obowiązków implementacyjnych w porządkach krajowych państw członkowskich. Lakoniczność wniosków, choć właściwych, sprawia, że uwadze Doktorantki umknęły zagadnienia merytoryczne mieszczące się w ramach sformułowanych we Wstępie hipotez 1-3 (s. 8)

- Po pierwsze, brakuje rozwinięcia kluczowego w tej kwestii pojęcia bezpieczeństwa narodowego (szczególnie w zestawieniu z szeroko definiowanymi innymi pojęciami, o których wcześniej była mowa w tej recenzji). Na str. 140 i n. mowa

jest o bezpieczeństwie państwa i bezpieczeństwie publicznym. Czy są to jednak pojęcia tożsame? Czy bezpieczeństwo państwa – wewnętrzne i zewnętrzne - obejmuje także ochronę praw i wolności jednostek? Czy bezpieczeństwo państwa związane jest i zależy od poszanowania wartości demokratycznych? Jeśli nie, skoro bezpieczeństwo państwa jest wartością chronioną także w państwach autorytarnych, to rozważania o konieczności zapewnienia prawnych standardów ochrony praw człowieka są na tak zakreślonym polu skazane na niepowodzenie. Za to rozróżnienie na bezpieczeństwo narodowe, publiczne i wewnętrzne ma zatem znaczenie. Znajduje także swoje implikacje w aktach prawa UE (w tym w TUE, TFUE, RODO i DODO).

- Po drugie, nie ma w ogóle mowy w tym miejscu pracy, ani też przy innej okazji (np. w pkt. dotyczącym organów nadzoru, s. 155; lub w obszernym omówieniu Polski), o nadzorze nad sposobem przetwarzania danych w trybie DODO sprawowanym przez służby, których zadania ustawowe mieszczą się w zakresie pojęcia bezpieczeństwa narodowego. W Polsce na podstawie ustawy z 14.12.2018r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nadzór ten został powierzony prezesom sądów wyższych instancji i Krajowej Radzie Sądownictwa (KRS). W tym zakresie nadzór nad działalnością sądów rejonowych sprawuje prezes sądu okręgowego, nad działalnością sądów okręgowych – prezes sądu apelacyjnego, natomiast nad działalnością sądów apelacyjnych – KRS (art. 175dd par. 1 ustawy). W konsekwencji, w ramach sprawowanego nadzoru nad sposobem przetwarzania danych osobowych, organy te mogą żądać dostępu do wszelkich danych osobowych w prowadzonych postępowaniach. W komentarzach do takiego rozwiązania prawnego pojawiły się wątpliwości, wyrażane m. in. przez RPO, A. Bodnara o zgodność z prawem UE, a w szczególności z KPP powstałe na gruncie potwierdzonym wyrokiem TSUE brakiem u niezależności KRS oraz wątpliwości co do niezależności od władzy wykonawczej prezesów sądów. Co z tego wynika dla Polski? Jakie są konsekwencje powierzenia nadzoru w przedmiotowym zakresie organom krajowym, które nie mogą być uznane za niezależne?

- Po trzecie, jeśli jak stwierdza Doktorantka, profilowanie, które zmierza do zapobieżenia aktowi terroryzmu lub wykrycia terrorysty, może nie być objęte przepisami DODO, w wyniku czego gwarancje ochrony praw człowieka w tym zakresie mogą zostać istotnie ograniczone, to jak ową lukę zapełnić, bez pełnej harmonizacji i

podporządkowania krajowych systemów ochrony danych prawu unijnemu, także formalnie, tj. w braku bezpośredniego stosowania i bezpośredniego skutku przepisów dyrektywy policyjnej? W szczególności, jak przedstawia się w tej sytuacji możliwość stosowania przepisów RODO?

Kolejne wątpliwości recenzenckie powstają w związku ze stwierdzeniem Autorki, że: „terroryzm może być przyczyną zawieszenia gwarancji ochrony praw człowieka zarówno w oparciu o system powszechny, jak i regionalny. Akty terroryzmu zagrażają bowiem wartościom chronionym przez umowy międzynarodowe. Wobec tak postawionej tezy należy rozważyć, czy profilowanie może zostać wykorzystane w ustawodawstwie proinwigilacyjnym motywowanym wzmożeniem ochrony jednostki, bezpieczeństwa państwa i przeciwdziałania terroryzmowi." (s. 143). Chodzi więc zasadniczo o ograniczenie praw i wolności osób podejrzanych o terroryzm, jak więc inwigilacja ma te prawa „wzmóc"? Inwigilacja ma wszak dotyczyć tej samej grupy osób. Przy okazji, niejasne jest jak Autorka rozumie termin inwigilacji i czym ta ostatnia różni się od profilowania? W kolejnym zdaniu w tym samym akapicie pada stwierdzenie o postulacie „ścisłej kontroli sądowej", ale bez wskazania na jakiej podstawie prawnej, w jakim trybie i w jakich warunkach odpowiedzialności prawnej.

Samym sednem problemu badawczego w recenzowanej rozprawie doktorskiej jest budowanie europejskiego standardu ochrony danych osobowych i prawa do prywatności, w Europie, ale także poza nią. Standard ten może mieć bowiem także zastosowanie do administratora danych lub podmiotu przetwarzającego, którego siedziba znajduje się poza UE. Jest to tzw. eksterytorialny, transgraniczny wymiar ochrony danych osobowych, o czym jest mowa na kartach tej pracy w pkt. 6 rozdziału II pt. „Przekazywanie danych osobowych do państw trzecich i organizacji międzynarodowych", zwany przez Doktorantkę „interoperacyjnością systemów informatycznych w UE" (UE/USA, Kanada, Chiny, tak na s. 121-128). Recenzowana rozprawa szczegółowo przedstawia istniejące powiązania organizacyjne i funkcjonalne, sukcesywnie ustanawiane, pogłębiane i poszerzane wraz z rozwojem nowych technologii, których skutek jest prawie zawsze transgraniczny. Postęp technologiczny sprawia, że we współczesnym świecie państwa nie są w stanie operować w oderwaniu i separacji. Skoro nie jest możliwe rozłączne funkcjonowanie, to państwa są niejako zmuszone do stałego wysiłku pogłębiania współpracy i budowania systemu ochrony

danych osobowych, tak by nadążyć za postępem technologicznym. Powstaje w ten sposób skoordynowana globalna przestrzeń prawna, w której poza ułatwieniami technicznymi i organizacyjnymi, przyjmowane są także standardy normatywne. Dzięki temu koszty związane z ochroną mogą zostać obniżone i ochrona ta staje się nie tylko bardziej skuteczna, ale i tańsza. Co jednak się dzieje, jeżeli państwo trzecie lub organizacja międzynarodowa nie zapewnia odpowiedniego stopnia ochrony? Jaki poziom może być uznany za „należyty" (tak na s. 123 rozprawy) w tak bardzo zróżnicowanych systemach prawnych? Jaki podmiot jest uprawniony do ceny poszanowania odpowiedniego standardu ochrony? Co w tej materii orzekł TSUE?

W recenzowanej rozprawie można także wskazać fragmenty, które należy uznać za szczególnie udane badawczo i o dużej wartości merytorycznej. Najlepiej opracowaną częścią pracy są rozdziały IV i V odpowiednio dotyczące zagrożeń i ryzyka związanych z profilowaniem oraz profilowania w praktyce. Autorka dokonuje rzetelnej, uporządkowanej, logicznej i spójnej analizy przedmiotowego problemu, na solidnej podstawie normatywnej, z szerokim odwołaniem do literatury naukowej i orzecznictwa sądów międzynarodowych i krajowych.

Formułując ostatecznie ogólną ocenę merytoryczną recenzowanej rozprawy należy stwierdzić, że jest ona **pozytywna**.

4. Ocena formalna pracy

Pod względem warsztatowym, praca nie wzbudza większych zastrzeżeń. Bibliografia i przypisy są zasadniczo sporządzone prawidłowo, chociaż zdarzają się usterki, jak. np. zaliczenie rezolucji ONZ (pkt 1.4 bibliografii) oraz rezolucji, zaleceń i programów wydanych przez instytucje UE (pkt 1.5) do aktów prawa, wskazanie obowiązującej wersji TUE i TFUE na podstawie Dz. Urz. z 2008 r., podczas gdy obowiązują teksty ujednolicone ze zmianami w wersji opublikowanej w 2016r. Uwaga ta dotyczy także KPP. We wszystkich odwołaniach do orzecznictwa TSUE oraz do opinii rzeczników generalnych oprócz nazw stron i sygnatury powinien być przywołany także nr ECLI. Bywa, że niektóre ustalenia dokonane są bez podania źródeł, tak np. na s. 145, 161 lub występują hybrydy językowe, jak np. powołanie „smart contractów" na s. 228.

Wątpliwości i uwagi krytyczne podniesione przy okazji oceny konstrukcji i systematyki pracy nie zmieniają ogólnej oceny, że badania w całej pracy prowadzone są sumiennie. Wartość naukową dysertacji znacznie podnosi jasne i czytelne zestawienie problemów teoretycznych z praktycznymi. Udokumentowanie pracy jest bardzo obszerne, wybór literatury i dokumentów można uznać za wyczerpujący.

5. Ostateczna konkluzja

Przedstawiona do recenzji rozprawa doktorska mgr. Aleksandry Kacały-Szwarczyńskiej spełnia wymagane prawem warunki, określone w art. 13 ustawy z dn. 14 marca 2003 r. o stopniach naukowych oraz o stopniach i tytule w zakresie sztuki w obowiązującej wersji (Dz. U. z 2017 r., poz. 1789 ze zm.) i na tej podstawie wnoszę o dopuszczenie jej do dalszego postępowania doktorskiego.

Dagmara Kornobis-Romanowska