Dr hab. Arwid Mednis
Wydział Prawa i Administracji
Uniwersytet Warszawski

Warszawa, 5 grudnia 2023 r.

Recenzja rozprawy doktorskiej
Pana magistra Piotra Siemieniaka pt. Ochrona danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych

Przedmiotem niniejszej recenzji jest rozprawa doktorska Pana Piotra Siemieniaka pt. "Ochrona danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych" napisana pod kierunkiem dr hab. Wojciecha Wiewiórowskiego.

W pierwszej kolejności należy bardzo pozytywnie ocenić wybór tematu pracy. Idea ochrony prywatności i ochrony danych osobowych w fazie projektowania nie jest wprawdzie nowa, ale w polskiej literaturze nie doczekała się jeszcze kompleksowego opracowania.

Brak ten może dziwić ponieważ obowiązek ochrony danych osobowych w fazie projektowania obowiązuje od 25 maja 2018 r., tj. od daty zastosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) („RODO"). Wprowadzenie w RODO obowiązku ochrony danych osobowych w fazie projektowania było znaczącą zmianą w stosunku do poprzedniego stanu prawnego, tj. dyrektywy 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 oraz opartej na niej polskiej ustawie o ochronie danych osobowych z 29 sierpnia 1997 r. Autor recenzowanej pracy słusznie podkreśla, że wprowadzenie tego obowiązku do przepisów prawa powszechnie obowiązującego, stanowiło ogromny krok naprzód w regulacji ochrony danych osobowych.

Autor w swojej pracy nie ograniczył się jedynie do opisu prawnych i pozaprawnych mechanizmów ochrony danych osobowych w fazie projektowania, ale podjął się oceny efektywności istniejących w tym zakresie rozwiązań. W tym celu postawił następujące pytania badawcze:

- Czy istnieje jednoznaczna metoda oceny prawidłowości implementacji przez administratorów danych dla modelu ochrony danych w fazie projektowania?
- Czy rozwiązania prawne w obszarze ochrony danych osobowych skutecznie uzupełniają model ochrony danych w fazie projektowania, aby zmaksymalizować jego efektywność jako instrumentu prawnego?
- Czy model ochrony danych w fazie projektowania jest potrzebny w systemie prawnym UE?
- Czy działania organów ochrony danych są wystarczające, aby stosowanie modelu ochrony danych w fazie projektowania było skuteczne?
- Czy model ochrony danych osobowych ma wpływ na ochronę praw i wolności osób fizycznych?
- Czy model ochrony danych w fazie projektowania jest skutecznym instrumentem prawnym ochrony danych osobowych?

W mojej ocenie pytania są trafnie sformułowane i pozwalają wszechstronnie ocenić przydatność i skuteczność omawianego mechanizmu ochrony danych w fazie projektowania.

Odpowiedź na postawione pytania wymagała analizy całokształtu zagadnień związanych z ochroną prywatności i ochroną danych osobowych, w szczególności przepisów prawa powszechnie obowiązującego, obowiązujących norm, standardów i ujęć teoretycznych dotyczących ochrony danych w fazie projektowania. Pod tym względem praca jest poprawnie zbudowana, argumentacja jest spójna i logiczna pomimo pewnych nieścisłości i niedociągnięć, o których będzie mowa w dalszej części recenzji.

Praca Pana Piotra Siemieniaka składa się ze wstępu, pięciu rozdziałów podzielonych na podrozdziały, oraz zakończenia.

Punktem wyjścia jest omówienie w rozdziale I koncepcji prawa do prywatności, następnie prawa do ochrony danych osobowych oraz – w dalszej kolejności - analiza relacji pomiędzy tymi prawami. Rozdział ma charakter wprowadzający, jego rolą jest naświetlenie szerokiego tła aksjologicznego i prawnego, włączając w to podstawowe akty międzynarodowe, europejskie

i polskie. Można go zatem potraktować jako spełnienie pewnego standardu w tego typu pracach, a jednocześnie stanowi bardzo rzetelne przedstawienie regulacyjnego tła instytucji będącej głównym tematem pracy.

W rozdziale II Autor przechodzi do omówienia koncepcji ochrony danych w fazie projektowania. Opisuje zarówno kolejne podejścia do regulacji prawnych odnoszące się do tej koncepcji oraz obowiązek ustanowiony w tym zakresie w RODO. Następnie opisuje teoretyczne ujęcie ochrony danych osobowych w fazie projektowania, aby w kolejnym punkcie powrócić do szczegółowego omówienia kształtu regulacji ww. obowiązku w art. 25 ust. 1 RODO. Istotnym elementem tego opisu jest również wyjaśnienie koncepcji domyślnej ochrony danych (*data protection by design*) będącej częścią regulacji zawartej w art. 25 RODO (domyślnej ochronie poświęcono ust. 2 tego artykułu) z jednoczesnym nawiązaniem do teoretycznej koncepcji *Systems Development Life Cycle* (SDLC).

Warto podkreślić, że art. 25 ust. 1 RODO nie tylko każe uwzględnić ochronę danych osobowych w fazie projektowania, ale również uzależnia sposób realizacji tego obowiązku od stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikającego z przetwarzania. Administratorzy zostali w przepisach RODO zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja lub szyfrowanie, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu objęcia przetwarzania niezbędnymi zabezpieczeniami, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

W treści obowiązku ochrony danych osobowych w fazie projektowania znalazło się zatem odwołanie do stanu wiedzy technicznej, przy czym „stan wiedzy technicznej" oznacza zarówno technologie oferujące lepszą ochronę prywatności, jak i te, które w prywatność ingerują. Dlatego bardzo ważnym elementem pracy jest szczegółowy opis technologii z obu tych zakresów, tj. technologii wzmacniających ochronę prywatności (Privacy-Enhancing Technologies, *PETs*) oraz technologii naruszających prywatność (Privacy-Invading Technologies, *PITs*). Jest to niewątpliwie ważny i bardzo potrzebny wątek pracy.

Ochrona danych osobowych w fazie projektowania wpisuje się w koncepcję, na której zbudowane jest RODO, a mianowicie podejście oparte na analizie ryzyka (*risk-based approach*), które w pewnym uproszczeniu polega na tym, że prawodawca odstępuje od szczegółowego wyliczenia konkretnych środków technologicznych i innych, służących

ochronie danych osobowych na rzecz sformułowania obowiązku administratora w zakresie identyfikacji i szacowania ryzyka, a następnie samodzielnego doboru odpowiednich środków mitygujących lub eliminujących zidentyfikowane ryzyko.

Dlatego tak ważna jest dokonana w pracy analiza kwestii technologicznych, które muszą być uwzględnione nie tylko w fazie projektowania, ale również – co słusznie podkreślono – w całym cyklu przetwarzania danych osobowych.

Rozdział III pracy zawiera bardzo interesujący przegląd wymogów wynikających z RODO w kontekście obowiązków ochrony danych w fazie projektowania i domyślnej ochrony danych osobowych. Autor słusznie wskazuje, że pomimo swojej nazwy, zasada ochrony danych osobowych w fazie projektowania obowiązuje również na pozostałych etapach przetwarzania danych.

W rozdziale IV Autor opisuje normy, standardy, którymi administrator może posłużyć się w procesie zabezpieczania przetwarzania przed naruszeniami praw i wolności podmiotów danych w fazie projektowania. Dodano także interesujący opis modeli oceny dojrzałości tego procesu. Rozdział ten jest szczególnie istotny z uwagi na to, że normy i standardy stanowią uszczegółowienie przebiegu procesu ochrony danych w fazie projektowania. Autor opisuje również rolę certyfikacji i kodeksów postępowania jako sposobów potwierdzania spełniania obowiązków wynikających z RODO.

Kluczowym z perspektywy tematu pracy i postawionych pytań badawczych jest rozdział V, w którym dokonano oceny modelu ochrony danych w fazie projektowania i domyślnej ochrony danych i sformułowano propozycje rozwiązań zmierzających do wzmocnienia skuteczności tej ochrony.

Propozycja rozszerzonego podejścia do ochrony danych w fazie projektowania została podzielona na trzy obszary:

- Ochrona praw podstawowych w fazie projektowania i zasada odpowiedzialnego wykorzystania technologii,
- Ochrona prywatności oraz ochrona danych w fazie projektowania w systemie prawa,
- Edukacja i standaryzacja w fazie projektowania.

Propozycje objęte ww. obszarami zawierają ciekawe rozwiązania, chociaż Autor niestety nie precyzuje sposobów (formy) ich wprowadzenia (nie wskazano bowiem czy chodzi o zmiany w przepisach prawa, innych normach, standardach, itp.), a co do niektórych z nich można mieć wątpliwości, czy nie da się tych rozwiązań zastosować w obecnym stanie prawnym (chyba, że

intencją Autora w tych przypadkach jest wola, aby te propozycje faktycznie stosować w szerszym zakresie w praktyce).

Odnośnie do pierwszego z wymienionych obszarów, Autor formułuje tezy związane z szerszym zastosowaniem zasad etycznych w fazie projektowania (*ethics by design*). Autor odwołuje się tu m. in. do zasad sformułowanych pod adresem systemów sztucznej inteligencji. Warto tu jednak zwrócić uwagę, że np. prawo do poszanowania prawo do wolności, godności oraz autonomia jednostki (które składają się na zasadę respektowania czynnika ludzkiego) są zasadniczym celem RODO, a ryzyko ich naruszenia powinno być brane pod uwagę na etapie projektowania czynności przetwarzania danych osobowych. Podobnie jest z niektórymi pozostałymi zasadami przytaczanymi przez Autora, takimi jak ochrona prywatności, rozliczalność i transparentność. Rozumiem zatem, że postulat Autora zmierza do wzmocnienia praktyki stosowania *data protection by design* poprzez odpowiednie uwzględnienie zasad etyki.

W drugim obszarze (ochrona prywatności oraz ochrona danych w fazie projektowania w systemie prawa) Autor formułuje postulat stosowania podejścia *data protection by design* oraz *privacy by design* w odniesieniu do procesu tworzenia prawa tak, aby modele te stały się integralną częścią procesów legislacyjnych państw członkowskich UE. Postulat obejmuje wzmocnienie kompetencji organów nadzorczych w ramach kontroli przestrzegania praw jednostki na etapie legislacyjnym. Postulat ten należy uznać za słuszny, chociaż w pewnym zakresie RODO przewiduje możliwość zastosowania *privacy by design* na etapie legislacji w ramach oceny skutków przetwarzania (art. 35 ust. 10 RODO) choć nie mamy tu do czynienia z obowiązkiem. Ponadto, warto zwrócić uwagę, że w ramach europejskiego procesu legislacyjnego kwestia ochrony podstawowych praw i wolności jest zawsze brana pod uwagę. Postulat Autora powinien być zatem rozważany w odniesieniu do krajowego procesu legislacyjnego.

Autor rekomenduje również objęcie procesem ochrony w fazie projektowania danych nieosobowych. Uzasadnia to tym, że wszelkiego rodzaju dane elektroniczne, które nie są danymi osobowymi oraz rozwiązania techniczne służące do przetwarzania danych nieosobowych (oraz osobowych) stanowią istotną wartość dla obszaru innowacyjności w dziedzinie technologii, rozwoju gospodarki oraz budowania społeczeństwa informacyjnego. Zdaniem Autora, nowoczesne rozwiązania również wymagają zapewnienia odpowiedniego poziomu bezpieczeństwa z uwagi na to, że mogą mieć pośredni lub też bezpośredni udział w przetwarzaniu danych osobowych lub wpływ na niepowiązane procesy przetwarzania danych osobowych. Postulat ten nie jest do końca jasno sformułowany, nie wiadomo bowiem czy

dotyczy on wszystkich danych nieosobowych czy tylko takich, które mogą zostać potencjalnie skojarzone z konkretnymi osobami. Autor jest jednak zdania, że celem rozszerzenia procesu ochrony w fazie projektowania na dane nieosobowe jest konieczność ochrony podstawowych praw i wolności. Postulat ten zostanie częściowo spełniony w akcie w sprawie sztucznej inteligencji, którego projekt został właśnie przyjęty w wyniku trilogu. Postulat Autora dotyczy legislacji zarówno unijnej jak i krajowej.

Trzeci obszar propozycji Autora dotyczy edukacji i standaryzacji.

Wskazuje on, że osiągnięcie wyższego poziomu zainteresowania modelem ochrony prywatności i ochrony danych w fazie projektowania będzie możliwe dopiero, gdy podmioty zobowiązane do stosowania tych koncepcji będą w posiadaniu odpowiednich zasobów ułatwiających wykorzystanie tych koncepcji w praktyce. Zdaniem Autora, problemy praktyczne dotyczą przede wszystkim istniejących problemów w systemach teleinformatycznych oraz przewidywania potencjalnych zagrożeń. Administratorzy danych zatem powinni mieć dostęp do szerokiego spektrum wzorców, dobrych praktyk, materiałów o charakterze edukacyjnym oraz technologii informatycznych. Jak rozumiem, postulat ten nie dotyczy zmian w prawie, lecz praktyki stosowania *privacy by design*. Propozycję należy ocenić pozytywnie, chociaż Autor nie precyzuje sposobów jej wdrożenia.

Bardzo ważny postulat dotyczy odpowiedniego przygotowania pracowników do realizowania ról wspomagających *privacy by design* oraz *data protection by design*. Autor wskazuje, że odpowiednio przeszkoleni programiści wraz z inżynierami ds. bezpieczeństwa są kluczowymi stronami dla procesu wsparcia „tłumaczenia" wymagań, modeli i mechanizmów na wymagania systemów teleinformatycznych. Ma to szczególnie ważne znaczenie – jak twierdzi - z uwagi na to, że prywatność oraz bezpieczeństwo są formułowane na wysokim poziomie abstrakcji, który sprawia, że ich rozumienie jest mniej niż oczywiste. Autor widzi więc potrzebę powstawania nowych zawodów typu *privacy engineer*, czy też *security engineer*, które byłyby zawodami o charakterze interdyscyplinarnym. Postulat ten wpisuje się w ogólny trend rozwoju zawodów związanych z cyberbezpieczeństwem. W tej dziedziny mamy bowiem do czynienia z poważnym brakiem specjalistów.

Kolejna propozycja wiąże się z edukacją w zakresie *privacy by design*. Autor nie ogranicza się tu jednak do kwestii samej edukacji. Postuluje, aby inicjatywy o charakterze edukacyjnym wiązać z wprowadzeniem efektywnych metod nauczania w postaci otwartych szkoleń, warsztatów, studium przypadków dotyczących praktycznego podejścia dla modelu *privacy* oraz *data protection by design*. Zwraca uwagę, że grupą docelową dla działań edukacyjnych nie

mogą być tylko osoby z najwyższego kierownictwa podmiotów i instytucji. Powinny być zauważone również role, które mają największy wpływ na ostateczny efekt związany z budową i implementacją systemu teleinformatycznego.

Dodatkową proponowaną w pracy kategorią działań zmierzających do zwiększania efektywności koncepcji *privacy by design* oraz *data protection by design* jest rozwój otwartych inicjatyw, które będą wspierały Privacy-Enhancing Technologies. Technologie powinny być rozwijane w modelu *open source*.

Autor stawia także na rozwój odpowiednich norm i dobrych praktyk z zakresu ochrony danych w fazie projektowania. Porusza również niezwykle ważną kwestię dostępności norm, wymagań biznesowych, dobrych praktyk i innych zasobów wiedzy.

Dodatkową, interesującą propozycją jest testowanie i modelowanie zagrożeń prywatności oraz dokonywania ustandaryzowanej i sformalizowanej oceny poziomu dojrzałości dla poziomu ochrony prywatności i ochrony danych w fazie projektowania.

Należy podkreślić, że niezależnie od końcowych wniosków Autora, praca zawiera szereg bardzo cennych uwag i spostrzeżeń, np. dotyczących ryzyk, których dotyczy RODO, zasady sumy pozytywnej, strategii wspierających koncepcję privacy by design i innych. W sposobie przedstawienia tematu i praktycznej strony stosowania tej koncepcji, widać dużą znajomość tematu i doświadczenie Autora z tego zakresu. W pracy słusznie podkreśla się, że standardy bezpieczeństwa informacji stosowane w celu zapewnienia cyberbezpieczeństwa mają zastosowanie również do ochrony danych osobowych, która powinna być traktowana jako element szeroko rozumianego bezpieczeństwa sieci i systemów informacyjnych.

Autor stawia m. in. tezę, że art. 25 nie jest w RODO niezbędny, a w przypadku jego braku można by było stosować „zamiennie" z art. 24 oraz art. 32 RODO (s. 273). Teza ta jest tyleż ciekawa co kontrowersyjna, zważywszy, że art. 24 dotyczy ogólnej zasady stosowania RODO, a art. 32 kwestii zabezpieczenia danych osobowych. W tym znaczeniu obowiązku określonego w artykule 25 RODO nie można traktować jako ekwiwalentu obu tych obowiązków, ponieważ dotyczy on w szczególności obowiązku zadbania o szeroko rozumiane bezpieczeństwo danych osobowych na etapie – jak wskazuje sama nazwa tego obowiązku – projektowania. Jak wynika z dalszej części rozważań, Autor przyznaje zresztą, że art. 25 RODO „promuje" działania na etapie projektowania.

Słuszna jest natomiast diagnoza Autora odnośnie do faktycznej roli kodeksów postępowania oraz mechanizmów certyfikacji. Nie spełniły one nadziei, jakie w nich pokładano, ponieważ

kodeksy pełnią rolę marginalną, natomiast mechanizm certyfikacji być może stanie się bardziej popularny dopiero wraz z wprowadzeniem nowych obowiązków w tym zakresie w przepisach dotyczących cyberbezpieczeństwa.

Metodyka zastosowana w pracy jest poprawna, Autor łączy elementy różnych metod z przewagą metody dogmatycznej. W pracy przeanalizowano również uwarunkowania historyczne regulacji prawnych z zakresu ochrony danych osobowych, sięgnięto do dobrych praktyk, norm i standardów, które mogą mieć charakter uzupełniający w stosunku do przepisów powszechnie obowiązujących, które regulują zagadnienie ochrony danych w fazie projektowania jedynie w sposób ogólny.

W pracy można dostrzec jednak pewne niedociągnięcia formalne.

Zabrakło na początku pracy wyraźnego ustalenia siatki pojęciowej, co skutkuje wrażeniem, że Autor używa tych samych terminów w różnych znaczeniach. Autor posługuje się często np. pojęciem „model", m. in. model *privacy by design*, model *data protection by design*, itp. W mojej ocenie należałoby przede wszystkim wskazać w jakim znaczeniu pojęcie „model" występuje w pracy. Model może być bowiem rozumiany jako system założeń, pojęć i zależności między nimi, pozwalający opisać (modelować) w przybliżony sposób jakiś aspekt rzeczywistości. Modelem może być także przedmiot badań, wzór, którego badanie pozwala otrzymywać informacje na temat rzeczywistości. Niezależnie od powyższego, należałoby doprecyzować, czy model *privacy by design* to np. koncepcja zaproponowana przez Ann Cavoukian, a co do modelu *data protection by design* – czy chodzi o jakąś koncepcję teoretyczną, czy też o kształt obowiązku opisany w art. 25 ust. 1 RODO. Podobna uwaga dotyczy pojęcia regulacji, które – jak można się domyślać - używane jest nie w znaczeniu aktów prawnych, ale raczej poszczególnych instytucji prawa ochrony danych (obowiązków administratorów i praw podmiotów danych). Pomimo wyjaśnienia (na s. 66) pojęcia „instrument" wydaje się, że Autor używa go zamiennie w znaczeniu praw podmiotowych i aktów prawnych. Szkoda także, że Autor nie sięgnął do koncepcji publicznych praw podmiotowych w odniesieniu do niektórych praw podmiotów danych.

Nie jest również jasne jak Autor widzi relację pomiędzy ochroną danych w fazie projektowania a domyślną ochroną danych. Ochrona domyślna zakłada przetwarzanie tylko niezbędnych danych osobowych, a zasada minimalizacji ma być jednym ze skutków realizacji koncepcji ochrony danych w fazie projektowania, niemniej brakuje tu jasności co do intencji Autora. W

niektórych fragmentach pracy odnosi się on tylko do ochrony w fazie projektowania, w innych omawia ją wraz z ochroną domyślną. Nie jest również jasne sformułowanie tytułu pracy, w którym „ochrona danych w fazie projektowania" (w liczbie pojedynczej) występuje jako „instrumenty prawnej ochrony" (w liczbie mnogiej). Być może pierwotnie Autor zamierzał ująć w temacie zarówno ochronę danych w fazie projektowania jak i ochronę domyślną, ewentualnie (być może) rozumie ochronę w fazie projektowania jako zestaw wymogów opisanych w rozdziale II w pkt 2.2. Kwestia ta w przypadku publikacji pracy wymagałaby korekty lub wyjaśnienia.

W świetle postawionych pytań badawczych należy stwierdzić, że Autor jedynie w ograniczonym zakresie poruszył kwestię kontroli obowiązku ochrony danych osobowych w fazie projektowania. Naruszenie tego obowiązku jest zagrożone administracyjną karą pieniężną, o której mowa w art. 83 ust. 4 lit. a) RODO. Zagadnienie to jest o tyle ważne, że w istocie omawiany obowiązek ma w dużej mierze charakter ocenny, a zatem bardzo ważne jest tu podejście organu nadzorczego do sposobu realizacji ww. obowiązku. Dodatkowo, ocena dokonana przez organ podlega w polskim systemie prawnym ocenie sądu administracyjnego, którego kontrola ogranicza się wyłącznie do kryterium legalności. Sąd administracyjny nie ma zatem możliwości kontroli poprawności wykonania obowiązku ochrony danych osobowych w fazie projektowania w świetle innych kryteriów (poprawności metodologicznej, zasadności, itp.). Dla pełnej oceny skuteczności tego modelu kontroli realizacji omawianego obowiązku należało w mojej ocenie dokonać głębszej analizy uprawnień zarówno organu nadzorczego jak i sądu.

Rozprawa doktorska Pana Piotra Siemieniaka jest napisana poprawnym i przejrzystym językiem. Zawiera nieliczne błędy literowe i edycyjne, nie wpływają one jednak na bardzo pozytywny odbiór pracy zarówno od strony językowej, jak i wizualnej. W przypadku publikacji należałoby w szczególności przeredagować wstęp pracy, który jest nieco chaotyczny i sprawia wrażenie napisanego dużo wcześniej, o czym świadczy traktowanie jako prognoz ilości danych na rynku w roku 2020, chociaż dysertacja została sporządzona według stanu na 2022 rok.

Należy również wysoko ocenić dobór literatury i orzecznictwa, są one szeroko powoływane i prawidłowo wykorzystane. W mojej ocenie, Autor nie pominął żadnej istotnej pozycji z omawianego zakresu.

Wnioski dysertacji odpowiadają postawionym na początku tezom.

Wnioski

Pomimo przedstawionych powyżej uwag stwierdzam, że w mojej ocenie, rozprawa doktorska Pana magistra Piotra Siemieniaka pt. Ochrona danych w fazie projektowania jako instrumenty prawnej ochrony danych osobowych spełnia wymogi określone w art. 13 ust. 1 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) i uprawnia do ubiegania się o nadanie stopnia naukowego doktora nauk społecznych w dyscyplinie nauki prawne. W szczególności, przedstawiona rozprawa doktorska, stanowi ważny wkład w naukę prawa ochrony danych osobowych, zawiera także ciekawe naukowo wnioski oraz propozycję rozwiązania przedstawionego problemu naukowego.

Przeanalizowany materiał, w tym przepisy prawa, stanowiska wyrażone w literaturze i orzecznictwie wskazują na dużą swobodę Autora w poruszaniu się w obrębie omawianej problematyki, a tym samym na dużą wiedzę teoretyczną z tego zakresu. Ponadto, praca porządkuje obecny stan wiedzy, ma zatem również walor edukacyjny. Z tego względu, rekomenduję jej publikację, po uwzględnieniu uwag zawartych w niniejszej recenzji.

Dr hab. Arwid Mednis