Karolina Gałęzowska
Wydział Prawa i Administracji
Uniwersytet Warszawski

AUTOREFERAT

pracy doktorskiej

„Kontrola transgranicznych procesów przetwarzania danych osobowych – problemy prawno-administracyjne”

Promotor:

Prof. dr hab. Jacek Jagielski
Wydział Prawa i Administracji
Uniwersytet Warszawski

Recenzenci:

dr hab. Paweł Fajgielski, prof. KUL
Wydział Prawa i Administracji
Katolicki Uniwersytet Lubelski

dr hab. Dariusz Szostek, prof. UŚ
Wydział Prawa i Administracji
Uniwersytet Śląski

Warszawa 2024

1. Uzasadnienie wyboru tematu pracy

Tematem pracy jest kontrola międzynarodowych (transgranicznych) procesów przetwarzania danych osobowych, tj. kontroli zgodności procesów przetwarzania danych przekazywanych poza teren Europejski Obszar Gospodarczy tj. do tzw. państw trzecich. Postępująca globalizacja gospodarki oraz rozwój usług cyfrowych wpływają na większy przepływ danych osobowych. Procesów tych nie sposób ograniczyć do terytorium jednego państwa. Ponadto, rozwijające się technologie analityczne oraz systemy sztucznej inteligencji wymagają dostępu do ogromnej ilości danych w tym danych osobowych, m. in. w celu trenowania tych systemów. W praktyce oznacza to transgraniczne wykorzystanie danych z zasobów Internetu i innych źródeł.

Unia Europejska z jednej strony dąży do zapewnienia obywatelom dostępu do nowoczesnych usług, z drugiej – zapewnienia wysokiego standardu ochrony praw podstawowych. Europejskie prawo ochrony danych osobowych jest istotnym elementem ochrony praw i wolności obywatelskich, które mogą zostać naruszone w związku z przetwarzaniem ww. danych. Na obecny, wysoki standard składają się m.in. uprawnienia podmiotów danych (m.in. dostęp, poprawienie treści błędnych danych), obowiązki w zakresie transparentności przetwarzania i bezpieczeństwa danych oraz obowiązek wyznaczenia właściwego organu nadzorczego. Istotnym zagadnieniem, przed którym stanął prawodawca europejski było zapewnienie tych standardów wobec danych osobowych transferowanych do państw trzecich. Rozporządzenie ogólne o ochronie danych osobowych[1] (Rozporządzenie 2016/679) zawiera szereg wymogów w tym zakresie, które odnoszą się do warunków transferu danych, jednakże przepisy te z oczywistych względów tylko pośrednio dotyczą odbiorców danych w państwie trzecim. Problemem jest bowiem skuteczność przyjętych rozwiązań w sytuacji terytorialnego ograniczenia stosowania przepisów Rozporządzenia 2016/679. Jednocześnie, warto zauważyć, że przepisy europejskie w tym zakresie są często inspiracją i wyznacznikiem dla innych państw; do pewnego stopnia traktowane są jako modelowe rozwiązanie. W związku z transferami danych do państw trzecich Unia aktywnie dąży do implementowania przez nie swojego modelu ochrony. Wiąże się z tym wiele wyzwań w sferze ekonomicznej i politycznej, a jednym z głównych wyzwań prawnych jest stworzenie modelu kontroli transferów danych osobowych.

[1] Dz. UE L 119 z 4.05.2016, str. 1–88.

Temat pracy uważam za istotny z uwagi na potencjalne zagrożenia praw podstawowych, w tym prawa do ochrony w związku z przetwarzaniem danych osobowych, prywatności czy prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu. Konsekwencje związane z przekazywaniem danych osobowych do państwa, które nie gwarantuje odpowiedniego stopnia ochrony tych praw, są bardzo dotkliwe. Jednocześnie postępowanie w przypadku transgranicznego przetwarzania, konieczność zapewnienia skutecznej kooperacji międzynarodowej i wskazania prawa właściwego powodują, że szczególnie zagadnienie kontroli administracyjnej jakie gwarancje zapewnił podmiot przekazujący dane osobowe do państwa trzeciego, dostarcza ciekawych problemów badawczych. Najistotniejszy z nich, w mojej ocenie, jest następujący: jak zapewnić bezpieczeństwo podmiotów danych w dobie globalnej cyfryzacji?

Wyzwanie to jest jednym z kluczowych dla Komisji Europejskiej. Do strategicznych celów Unii w obszarze cyfryzacji należy m.in. tworzenie bezpiecznych przestrzeni cyfrowych w ramach Europejskiej agendy cyfrowej. W strategii z 2020 roku, która miała na celu kształtowanie cyfrowej przyszłości Europy, skoncentrowano się na technologiach, które przynoszą korzyści ludziom, konkurencyjnej gospodarce oraz otwartemu, demokratycznemu społeczeństwu. W 2021 roku strategia ta została wzbogacona o cyfrowy kompas na 2030 rok, w którym określono cele UE w zakresie cyfryzacji na kolejną dekadę[2]. Cele te obejmują m.in. wzrost kompetencji cyfrowych, zwiększenie udziału usług cyfrowych w administracji publicznej oraz korzystanie przez przynajmniej 75% przedsiębiorców z usług w chmurze, dużych zbiorów danych i sztucznej inteligencji.

W centrum tych strategicznych ambicji i planów jest wykorzystywanie danych, w tym danych osobowych, bowiem nowoczesne technologie cyfrowe zwykle wymagają przetwarzania transgranicznego, czyli takiego, w którym dochodzi do przetwarzania danych obywateli różnych państw w ramach jednej usługi. Transfery danych osobowych do państw trzecich, które mają odmienne od unijnych standardy ochrony w związku z przetwarzaniem danych osobowych, wiążą się jednak z ingerencją w prawo do prywatności i inne prawa jednostki; ingerencja ta powoduje konieczność przyjęcia określonych zasad normatywnych, technicznych i organizacyjnych dla transferów, mitygujących zagrożenia, jakie powodują. Unijne przepisy dotyczące przekazywania danych od tych państw wymagają zapewnienia odpowiedniego, ekwiwalentnego standardu ochrony.

[2] Źródło: https://www.europarl.europa.eu/factsheets/pl/sheet/64/digital-agenda-for-europe.

Równolegle pojawiają się głosy wskazujące, że cel w postaci zagwarantowania odpowiedniego poziomu ochrony został w dużej mierze osiągnięty. Obecnie w ponad 150 jurysdykcjach[3] przyjęto ustawodawstwo dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Wiele z nich opartych jest w dużym stopniu na wzorze europejskim, głównie Rozporządzeniu 2016/679. Akt ten szczegółowo reguluje zasady przetwarzania danych osobowych, jego podstawy prawne i obowiązki, jakie spoczywają na administratorach. Przepisy Rozporządzenia 2016/679 są jednak szczególne w porównaniu ze swoimi odpowiednikami. Duże znaczenie ma w nich, poza uprawnieniami podmiotów danych, rozliczalność administratorów (rozumiana jako umiejętność wykazania zgodności przetwarzania z odpowiednimi normami) i organów ich kontrolujących. Rozliczalność tę, podobnie jak w przypadku ochrony innych praw podstawowych KPP UE, zapewniają instytucje prawa administracyjnego, w tym w szczególności zapewnienie podmiotom danych prawa do skutecznego środka odwoławczego wobec decyzji. Przepisy Rozporządzenia 2016/679 niosą również wymóg powołania właściwego organu nadzoru, odpowiedzialnego m.in. za kontrolę przestrzegania zasad przetwarzania danych. Standard europejski jest więc wielowymiarowy i zapewnia ingerencję państwa w przypadku, w którym dochodzi do nieprawidłowości w związku z przetwarzaniem danych.

Nie sposób jednak instytucji zawartych w Rozporządzeniu 2016/679 porównać do rozwiązań państw trzecich, spoza EOG, mających odmienne tradycje prawne. Co jednak najistotniejsze z perspektywy tematu pracy, nie sposób też nie zwrócić uwagi na lakoniczne poruszenie kwestii nadzoru i kontroli w przypadku przekazywania danych do państw trzecich. Trudno bowiem, szczególnie w sferze prawa administracyjnego, postawić wymóg zapewnienia odpowiedniego poziomu ochrony, pozbawiwszy jednocześnie podmioty danych skutecznych środków ochrony.

Sposoby zapewnienia tego ekwiwalentnego poziomu są niekiedy pomocniczo sugerowane przez Trybunał Sprawiedliwości Unii Europejskiej (TS). To właśnie Trybunał przyjął interpretację wymuszającą wprost zapewnienie ochrony nie tyle nawet adekwatnej do zagrożeń, co w istocie odpowiadającej wzorcowi europejskiemu w przypadku transferów danych. TS, szukając sposobów na skuteczne zrealizowanie celów wprost wskazanych w Rozporządzeniu 2016/679 oraz ochrony praw podstawowych obywateli UE, skupia się jednak na rozwiązaniach formalistycznych, nie mogących znacząco wpłynąć na sytuację podmiotu danych, np. przeprowadzenie dodatkowych analiz ryzyka. Tym większe wątpliwości wzbudza

[3] G. Greenleaf, *Countries with Data Privacy Laws – By Year 1973-2016 (Tables)*, „146 Privacy Laws & Business International Report" 2017, no. 18, SSRN: https://ssrn.com/abstract=2996139.

możliwość realizacji postulatu zapewnienia ekwiwalentnego poziomu ochrony podmiotom danych.

Należy przyznać, że zadanie to nie jest jednak łatwe do zrealizowania. Zapewnienie odpowiedniego poziomu ochrony na podstawie norm publicznoprawnych w państwach Unii i poza nią, wymaga dużej międzynarodowej kooperacji. Dążenie do niego jest jednak niezbędne dla celów, jakie obecnie stawia sobie Europa. Transfery do państwa nieposiadającego odpowiedniego poziomu ochrony danych osobowych bowiem mogą w istocie nieść za sobą wiele rodzajów ryzyka, m.in. poprzez naruszenie prywatności, kradzież danych czy nieautoryzowany dostęp do nich. W konsekwencji szczególnie dla tych operacji przetwarzania danych osobowych istnieje potrzeba przyjęcia właściwego modelu kontroli administracyjnej.

W pracy zadałam też pytanie dotyczące tego, jak precyzyjnie zdefiniowany jest cel europejskich przepisów: czy w przypadku transferów do państw trzecich faktycznie poziom ochrony ma być zbliżony, ekwiwalenty czy może identyczny z tym, jaki gwarantują instytucje Rozporządzenia 2016/679? Wciąż zasadne jest, w mojej ocenie, pochylenie się nad celowością i zakresem ingerencji w ochronę praw podmiotów danych po przekazaniu ich danych do państw trzecich.

Dodatkowo o aktualności problemu świadczy szeroko komentowane i krytykowane porozumienie wypracowane w lipcu 2023 r.[4] między UE a USA, dotyczące transferów danych osobowych z UE do tego państwa. Porozumienie to dotyczy uznania adekwatności ochrony dla transferów do wybranych podmiotów w USA, przystępujących do *Privacy Framework*. Z uwagi na szeroko komentowane programy inwigilacyjne tego państwa, porozumienie wypracowane przez Komisję najpewniej podzieli los swoich poprzedników: podobnych porozumień, które przez TS były uznawane za nieważne, głównie z uwagi na niesatysfakcjonujący poziom ochrony praw podstawowych. Jednocześnie, pomimo braku ustawy federalnej, poszczególne stany przyjmują lokalne regulacje w dużej mierze zbliżone do Rozporządzenia 2016/679, co wskazuje na duże znaczenie standardów europejskich.

Podsumowując, temat pracy nie doczekał się kompleksowego opracowania w doktrynie polskiej, a z uwagi na postępujące zmiany cywilizacyjne jest nadzwyczaj aktualny.

2. Cele i główne problemy badawcze poruszone w rozprawie

Podstawowym celem pracy było szczegółowe omówienie sytuacji prawnej osoby fizycznej, której dane są przekazywane do państw trzecich, i porównanie jej do sytuacji osoby, której dane

[4] Informację o sukcesie negocjacyjnym podano ok. miesiąc przed złożeniem pracy.

nie są przekazywane do państw trzecich. Analizę tę ograniczyłam do norm prawno-administracyjnych, z uwagi na wybrany temat pracy. Szczególną rolę w mojej analizie ma koncepcja publicznych praw podmiotowych. W przypadku bowiem prawa do ochrony w związku z przetwarzaniem danych osobowych, dorobek polskiej doktryny wskazuje jednoznacznie, jaka jest sytuacja podmiotu danych (osoby, której dane dotyczą) w relacji z polskim organem nadzorczym[5]. Podmiot danych ma możliwość skierowania żądania określonej treści, a organ jest zobowiązany do jego realizacji. W przypadku transferów do państw trzecich wydaje się, że sytuacja jest odmienna – podmiot danych ma zapewnione formalnie te same uprawnienia, choć tylko w przypadku, w którym Rozporządzenie 2016/679 ma w ogóle zastosowanie. Nawet jednak w tych przypadkach uprawnienia podmiotu są z natury formalne, nie istnieją bowiem środki ochrony prawnej wobec naruszenia dokonanego w państwie trzecim. Organ nadzorczy nie dysponuje środkami nadzoru wobec takich administratorów. W konsekwencji poziom ochrony osób fizycznych doznaje uszczerbku.

Na tej podstawie jako główną tezę pracy przyjęłam, że obecnie przyjęte środki ochrony prawnej nie są wystarczające do zapewnienia jednakowego poziomu ochrony w przypadku transferu danych. Szczególnie, że w przypadku transferu do państwa trzeciego prawo do ochrony danych osobowych przestaje być publicznym prawem podmiotowym. Powyższą główną tezę badawczą uzupełniają dalsze, pomocnicze tezy szczegółowe pracy:

1) dla zapewnienia ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych właściwe są regulacje prawno-administracyjne; w praktyce zapewniają skuteczniejszą ochronę. Cywilnoprawna ochrona danych osobowych słusznie uznana została za niewystarczającą, m.in. z uwagi na wymóg udowodnienia istnienia zagrożenia prawa lub wręcz udowodnienia samego naruszenia oraz ewentualnej szkody;

2) na podstawie istniejącego dorobku judykatury, w tym w szczególności dorobku TS, należy uznać materialny zakres ochrony za bardzo szeroki. Większość informacji stanowi dane osobowe i w praktyce wydaje się, iż trudniejszym zadaniem jest udowodnienie, że określone informacje nie stanowią danych osobowych;

3) w historii rozwoju regulacji dotyczących danych osobowych da się zauważyć tendencję do rozszerzania i uszczegóławiania zasad ochrony prywatności w związku z przetwarzaniem danych osobowych oraz powoływania specjalistycznych organów nadzorczych i wyposażania ich w szerokie uprawnienia. Na przykładzie ochrony danych osobowych można zauważyć, że za wzrostem znaczenia czy konieczności ochrony danego dobra idzie zwiększanie ingerencji

[5] Tak: A. Mednis*, Prawo do prywatności a interes publiczny,* Kraków 2006.

władz publicznych w jego ochronę, a rozwiązania, w których za przestrzeganie określonych norm odpowiada specjalistyczny organ, uznawane są często za skuteczniejsze;

4) sama kwestia przekazywania danych do państw trzecich pozostawała dotąd poza głównymi rozważaniami na temat ochrony danych osobowych i egzekwowania przepisów dotyczących ochrony danych osobowych, a akty prawne chroniące prywatność nie regulowały precyzyjnie transferów;

5) obecnie formalne wymagania w przypadku oceny transferu – tzw. *Transfer Impact Assessment* (TIA), obejmują kompleksowe badanie zagrożeń związanych z przekazaniem do państw trzecich. Ocena ta pozostawiona jest w praktyce do samodzielnego wykonania przez podmioty sektora prywatnego, przez co nie może stanowić efektywnej formy ochrony.

Na marginesie powyższych rozważań zwróciłam uwagę na częste używanie w kontekście polskiego organu nadzoru – Prezesa Urzędu Ochrony Danych Osobowych (PUODO) – terminu „organ regulacyjny" lub „regulator". Omówiłam w pracy znaczenie tego pojęcia i przeanalizowałam status organów ds. ochrony danych osobowych, który różni się w stosunku do organów regulacyjnych, takich jak Komisja Nadzoru Finansowego czy Prezes Urzędu Komunikacji Elektronicznej. Udowodniłam, że określenie PUODO mianem organu regulacyjnego nie jest prawidłowe.

3. Metody badawcze

Opracowanie przedstawionych wyżej zagadnień w ramach pracy wymagało zastosowania przede wszystkim metody dogmatyczno-prawnej i teoretyczno-prawnej. Stanowią one podstawowe metody badawcze stosowane w badaniach z zakresu nauk prawnych. W największym stopniu wykorzystałam metodę dogmatyczną poprzez wykładnię i interpretację norm prawa na podstawie analizy obowiązujących przepisów (a w ograniczonym zakresie również ich poprzedników, w celu wykazania kierunku ewolucji instytucji prawa ochrony danych osobowych). Metoda ta wymagała również dokonania analizy wypowiedzi doktryny i orzecznictwa.

W pracy, przyjmując za podstawę prawo pozytywne, usystematyzowałam, tj. uporządkowałam materiał prawny, objaśniłam znaczenia przepisów oraz ustaliłam zasady i wytyczne przenikające prawodawstwo w zakresie transferów danych osobowych. Następnie przeprowadziłam analizę poglądów doktryny, ze szczególnym uwzględnieniem uzasadnienia aksjologicznego omawianych instytucji. W bardzo dużym stopniu omówiłam orzecznictwo,

wskazując na ewentualne luki i nieścisłości oraz do pewnego stopnia prawotwórczą rolę judykatury. Jest to szczególnie istotne przy orzecznictwie TS, z uwagi na pozycję Trybunału.

W ramach badań posłużyłam się niekiedy posiłkowo metodą komparatystyczną, porównując przyjęte obecnie modele kontroli do tych obowiązujących poza UE, oraz metodą historyczną w zakresie wyjaśnienia historii opisywanych instytucji. Biorąc pod uwagę, że przedmiotem badania jest materiał normatywny, jedynie uzupełniająco odniosłam się do praktyki funkcjonowania przepisów, choć poczyniłam też na ten temat uwagi.

4. Struktura pracy

W celu weryfikacji tez przeprowadziłam rozważania w ramach sześciu rozdziałów rozprawy oraz postawiłam szczegółowe hipotezy i pytania badawcze w każdym z nich.

W rozdziale I przedstawiłam wprowadzenie do problematyki ochrony prywatności i ochrony danych osobowych, zarys ich znaczenia historycznie oraz istotę we współczesnym świecie. Omówiłam w nim także znaczenie koncepcji publicznych praw podmiotowych oraz porównałam prawno-administracyjną ochronę do ochrony prawnocywilnej.

Z uwagi na analizę materiału normatywnego nie skupiłam się w pracy na konkretnych technikach czy sposobach przetwarzania danych osobowych i nie przeprowadziłam pogłębionej analizy wykorzystania danych osobowych w ramach uczenia maszynowego czy sztucznej inteligencji. Jednym z najistotniejszych elementów tego rozdziału było ukazanie, jak szeroki jest zakres przyjmowanej obecnie w judykaturze interpretacji pojęcia danych osobowych. Ma to swoje ogromne znaczenie dla przedmiotu pracy, gdyż przy okazji rozważań na temat najnowszych sporów interpretacyjnych wskazałam, że w praktyce, kiedy dochodzi do przetwarzania danych w jakikolwiek sposób wcześniej powiązanych z osobami fizycznymi, większym wyzwaniem jest wykazanie, że nie stanowią już danych osobowych. Obecnie obowiązujące przepisy traktują w odmienny sposób dane skutecznie zanonimizowane (np. zagregowane dane statystyczne), niemniej pieczę nad nimi sprawuje ten podmiot, który dane przetwarza. Dotyczy to także obowiązku oceny odwrócenia procesu anonimizacji i wtórnego przyporządkowania informacji do osoby fizycznej. W konsekwencji większość informacji przesyłanych między UE a państwami trzecimi wymaga przyjęcia reżimu właściwego dla ochrony danych osobowych.

Omówiłam ponadto prawo do ochrony danych osobowych jako publiczne prawo podmiotowe. W przypadku ochrony danych osobowych istnieje wymierny cel gospodarczy w takim ukształtowaniu praw podmiotów, aby ochrona ta była skuteczna. Jednocześnie jest to

także niezbędne z punktu widzenia zapewnienia skutecznej ochrony tego prawa podstawowego, co przynajmniej częściowo leży w interesie publicznym.

W rozdziale I dodatkowo rozważyłam powody i zasadność oparcia ochrony prywatności w aspekcie przetwarzania danych osobowych o normy prawno-administracyjne. Jak wskazałam bowiem we wstępie, początkowym punktem rozważań nauki prawa na temat ochrony prywatności było orzecznictwo cywilne w Stanach Zjednoczonych. W dalszym ciągu ochrona prywatności, m.in. w zakresie czci, miru domowego czy dobrego imienia, oparta jest o normy prawa cywilnego. W przypadku prawa do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, obecnie wyodrębnionego, za zasadne należy przyjąć rozwiązanie prawno-administracyjne. Przetwarzanie danych osobowych ma wymiar bardziej obiektywny niż obraza np. czci; może ponadto prowadzić do naruszeń na masową skalę. Wymaga też, z uwagi na silną pozycję administratorów, interwencji państwa.

W rozdziale II dokonałam przeglądu aktów prawnych dotyczących ochrony prywatności i ochrony danych osobowych, pokazałam ich rozwój oraz wyraźną tendencję do wyboru prawno-administracyjnych środków ochrony.

Podobne przeglądy aktów prawnych często pojawiają się w pracach poświęconych ochronie danych osobowych, niemniej w tym wypadku przegląd jest wykonany z perspektywy oceny rozwoju środków ochrony jednostki, powołania specjalistycznych organów kontroli oraz zasad dotyczących transferów danych do państw trzecich.

W omówionych przeze mnie aktach początkowo prawo do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych traktowano jako element prawa do ochrony prywatności. Pierwsze omówione przeze mnie akty prawne nie miały też mocy wiążącej. Z czasem doszło do wyodrębnienia w przepisach prawa do ochrony danych osobowych, co spotkało się z aprobatą przedstawicieli nauki[6]. Prawa te mają odrębne znaczenie i wiążą się z różnymi uprawnieniami. Z drugiej strony, co równie istotne, doszło do wskazania pewnego minimum ochrony, które jest najlepiej wyrażone w Konwencji 108 oraz wytycznych OECD – na tych przepisach wzorowane są przepisy innych państw. Obecnie za standard przyjmowane jest m.in.: nadanie podmiotom danych uprawnień informacyjnych; nałożenie obowiązku zapewnienia bezpieczeństwa przetwarzania; wyposażenie podmiotów danych w uprawnienia pozwalające na kontrolę prawidłowości przetwarzania danych; wymóg zbadania proporcjonalności przetwarzania danych w stosunku do celów; konieczność

[6] Szerzej: O. Lynskey, *Deconstructing data protection: the 'Added-value' of a right to data protection in the EU legal order*, „International and Comparative Law Quarterly" 2014, 63 (3), s. 569–597, doi:10.1017/S0020589314000244 [dostęp: 10.02.2024].

wskazania w prawie przesłanek legalizujących przetwarzanie danych oraz wykazania, że podstawa prawna przetwarzania jest precyzyjna i zrozumiała; powołanie niezależnego organu ds. ochrony danych osobowych oraz wreszcie wskazanie zasad przekazywania danych do państw trzecich.

W rozdziale III omówiłam szczegółowo zasady przekazywania danych do państw trzecich, zarówno historyczne, jak i obowiązujące na kanwie obecnych unijnych przepisów. Zasady te różnią się w zależności od tego, czy dochodzi do przekazywania danych do państw należących do państw Europejskiego Obszaru Gospodarczego (EOG), czy spoza EOG.

Mając na uwadze rozważania poczynione w rozdziale poprzedzającym, szczególnie w zakresie zapewnienia minimum ochrony, opisałam obowiązujące zasady przetwarzania danych w tych przypadkach, w których dochodzi do transferu do państwa trzeciego. W rozdziale dokonałam szczegółowego opisu modelu terytorialnego i hybrydowego oraz obowiązków administratorów, jakie wiążą się z obydwoma modelami. Pojawiający się w obu wymóg oceny adekwatności ochrony, zapewnianej przez państwo trzecie, prowadzi w istocie do konieczności przygotowania kompleksowego studium uwarunkowań prawnych ocenianego państwa. Poddane analizie muszą zostać normy konstytucyjne, szczegółowe przepisy w zakresie ochrony danych osobowych oraz dostępność i skuteczność środków ochrony prawnej. W przypadku legalizacji transferów do państw, które nie zapewniają ekwiwalentnego poziomu ochrony, dotychczasowe doświadczenia pokazują w szczególności słabość stosowanego modelu hybrydowego, w którym ocena ta pozostawiona jest podmiotom sektora prywatnego.

W rozdziale położyłam szczególny nacisk na źródło obowiązku objęcia ochroną danych w przypadku transferów do państw trzecich. Są to nie tylko przepisy unijne w zakresie ochrony danych osobowych, ale także KPP UE czy Konwencja.

Dodatkowo w rozdziale poddałam szczegółowej analizie najnowszą decyzję w sprawie Stanów Zjednoczonych. Pomimo że decyzja ta została dopiero co wydana, do TS wpłynęły już skargi związane z niezapewnieniem przez Stany Zjednoczone ekwiwalentnego poziomu ochrony. Choć skargi te zapewne nie doczekają się rozpatrzenia przez TS jeszcze w tym roku, dość powszechne jest przekonanie, że decyzja zostanie unieważniona, pomimo wysiłku Komisji, aby zbliżyć standardy ochrony w USA i UE. Przykład ten dobrze ilustruje niedoskonałości modelu terytorialnego.

Negatywnym skutkiem związanym z przekazywaniem danych do państw trzecich potencjalnie może być osłabienie standardu ochrony danych osobowych w porównaniu do ochrony, jaką cieszy się podmiot danych, kiedy jego dane pozostają fizycznie na terenie EOG.

W rozdziale IV dokonałam analizy znaczenia ochrony instytucjonalnej, bowiem istnienie odpowiednio umocowanego i niezależnego organu nadzorczego, właściwego w sprawach ochrony danych osobowych, ma kluczowe znaczenie dla ochrony podmiotów danych.

Ochrona instytucjonalna wiąże się z dalekim zaangażowaniem państwa w ochronę danego prawa. Konieczność powołania wyspecjalizowanych organów ds. ochrony danych osobowych jest konsekwentnie podkreślana od kilku dekad, czy to przy ocenie adekwatności prawa ochrony danych w państwach trzecich, czy w kolejnych aktach prawnych dotyczących ochrony danych. Wyodrębnienie zadań związanych z ochroną prywatności i przypisanie ich do niezależnego organu ma zapewnić łatwe i skuteczne egzekwowanie praw i kontrolowanie przetwarzania danych.

Przenosząc jednak te rozważania na grunt transferów danych do państw trzecich, zwróciłam uwagę, że w żadnym z obowiązujących modeli przekazywania danych do państwa trzeciego europejski organ ds. ochrony danych osobowych nie ma kompetencji do prowadzenia kontroli na terytorium państwa trzeciego. W konsekwencji kontrola i możliwość egzekwowania obowiązków w przypadku przetwarzania danych w państwie trzecim doznaje poważnego uszczerbku; w zasadzie pozostaje w dużej mierze kontrolą czysto formalną.

W rozdziale V omówiłam środki ochrony materialno-prawnej w przypadku transferu danych osobowych do państwa trzeciego. Środki ochrony prawnej dla przetwarzania danych na terenie EOG różnią się od środków ochrony danych, jakie można wykorzystywać w przypadku przekazywania danych do państwa trzeciego.

Istotnym dla pracy jest rozstrzygnięcie, czy w przypadku transferów danych wciąż mamy do czynienia z publicznym prawem podmiotowym. Publiczne prawa podmiotowe opisują takie relacje z organem administracji, w których jest on związany prawem, a jednostka może oczekiwać na tej podstawie realizacji określonych, wynikających z normy materialnej, uprawnień. Jest to zatem taka sytuacja jednostki, w której, na podstawie normy prawno-administracyjnej, jednostka może skutecznie domagać się czegoś od państwa lub może w sposób niezakłócony przez państwo zrealizować swój interes[7]. Odpowiednie gwarancje

[7] Za: R. Stankiewicz, *Publiczne prawa podmiotowe* [w:] *Prawo administracyjne,* J. Jagielski, M. Wierzbowski (red.), Warszawa 2022, s. 172–175.

procesowe, tzn. zapewnienie możliwości wykonywania kontroli, są kluczowe dla zapewnienia wysokiego poziomu ochrony danego prawa. W przypadku transferów danych natomiast realizacja żądania (czy roszczenia, jak przyjmuje się w literaturze dotyczącej publicznych praw podmiotowych) uzależniona jest nie tylko od organu nadzorczego, do którego zwraca się osoba zainteresowana (podmiot danych). Jeśli bowiem dane przesyłamy do państwa trzeciego, poza EOG, *de facto* roszczenie jest skierowane do podmiotów w tym państwie trzecim i aby to roszczenie zrealizować, potrzebne jest do tego wyposażenie podmiotów danych oraz organy ds. ochrony danych osobowych w odpowiednie instrumenty.

Rozdział VI poświeciłam natomiast na ocenę międzynarodowej współpracy na rzecz ochrony danych oraz rozważyłam kierunki rozwoju tej współpracy w przyszłości. W przypadku transferów nie jest możliwe zapewnienie ochrony danych osobowych bez współpracy z partnerami na terenie EOG czy w innych krajach. Obecnie jednak współpraca w tym zakresie jest z jednej strony szeroka, patrząc z perspektywy politycznych celów, jakie stawia sobie UE, z drugiej strony wciąż niewystarczająca w ocenie Trybunału Sprawiedliwości.

Całość rozprawy została zwieńczona zwięzłym podsumowaniem wniosków i wyzwań oraz bibliografią.

5. Najważniejsze wnioski

Realizacja postawionych celów badawczych stanowiła podstawę oceny obowiązującego modelu ochrony podmiotów danych w przypadku transferów i sformułowania wniosków *de lege ferenda* oraz *de sententia ferenda.* Dokonana analiza potwierdziła przyjętą dla rozprawy tezę o braku odpowiednich środków ochrony dla transferów danych oraz wskazała na konieczność powrotu do dyskusji na temat założeń systemu ochrony danych osobowych w Europie. W pracy zaproponowałam szereg rozwiązań, na których można w przyszłości oprzeć nowy model kontroli transferów. Ponadto poddałam krytycznej analizie eurocentryczność obecnego podejścia do kontroli transferów, w dużej mierze preferującego ścisłe odwzorowanie standardu europejskiego.