Przegląd Prawniczy
TBSP UJ 2020/2
ISSN 1689–9601

Martyna Gruszka[1]

Nowe zasady transferu danych osobowych z Unii Europejskiej do państw trzecich (wybrane zagadnienia)

Streszczenie:

Artykuł stanowi analizę najciekawszych zmian w regulacjach prawnych, dotyczących transferu danych osobowych z obszaru Unii Europejskiej do państw trzecich, z ostatnich kilku lat. W pracy omówione zostały niektóre reformy wprowadzone przez RODO, takie jak objęcie regulacją procesorów danych, problem transferów dalszych, a także transfer na podstawie wyjątków przewidzianych w rozporządzeniu. W dalszej części analizy przedstawiono skutki orzecznictwa Trybunału Sprawiedliwości w sprawie M. Schrems, w zakresie komercyjnego przekazu danych osobowych z Unii Europejskiej do Stanów Zjednoczonych.

Słowa kluczowe: RODO, ochrona danych osobowych, transfer danych osobowych z Unii Europejskiej, Tarcza Prywatności, Prawo UE

New Rules for the Transfer of Personal Data from the European Union to Third Countries (Selected Issues)

The article is an analysis of the most interesting changes in legal regulations regarding the transfer of personal data from the European Union to third countries. The paper discusses some reforms introduced by the GDPR, such as covering data processors, the problem of further transfers, as well as transfers based on the exceptions provided in the Regulation. The second part of the analysis presents the effects of the jurisprudence of the Court

[1] Autorka jest studentką III roku prawa na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego w Krakowie oraz absolwentką kierunku prawo własności intelektualnej i nowych mediów (I stopnia) na Wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego, martynagruszka@gmail.com, ORCID 0000–0002–2849–1812.

of Justice in the case of M. Schrems regarding the commercial transfer of personal data from the European Union to the United States.

Key words: GDPR, personal data protection, transfer of personal data from the European Union, Privacy Shield, EU Law

1. Wstęp

W erze cyfryzacji, globalizacji oraz rozwoju technologicznego ilość danych przetwarzanych oraz przekazywanych pomiędzy przedsiębiorstwami, podmiotami publicznymi, organizacjami międzynarodowymi czy poszczególnymi państwami stale rośnie. Powstanie i rozwój usług chmurowych (ang. *cloud computing*), komunikatorów internetowych, mediów społecznościowych, a także popularyzacja handlu elektronicznego zwiększa zaangażowanie w komercyjne transgraniczne operacje na danych ze strony przedsiębiorców czy jednostek. Powstaje potrzeba zapewnienia możliwości niezakłóconego przekazywania danych pomiędzy państwami i dostępu do tych danych bez względu na ich lokalizację. Z drugiej strony widnieje konieczność właściwego zabezpieczenia sfery prywatności obywateli unijnych oraz zachowania ich autonomii informacyjnej, rozumianej jako prawo do decydowania o zakresie udostępnianych w cyberprzestrzeni informacji. Autonomia informacyjna nie będzie bowiem pełna, jeżeli jednostka zostanie pozbawiona kontroli nad obiegiem informacji na jej temat[2]. Operacje transgranicznego transferu danych osobowych w dzisiejszych czasach są często skomplikowane, gdyż uwzględniają udział licznych urządzeń i podmiotów, których prawna kwalifikacja powoduje wątpliwości. Aby odpowiednio kontrolować prywatność informacji w cyberprzestrzeni, nie wystarczy wiedzieć, komu zostały one udostępnione, ale i komu informacje te udostępnił operator wykorzystywanej e-usługi.

Jak wskazuje Komisja Europejska, według stanu z maja 2016 r. na Unię Europejską przypadało tylko 4% całkowitej kapitalizacji największych platform internetowych[3]. Kluczowe jest zatem określenie, na ile prawo unijne zabezpiecza użytkowników europejskich nie tylko, gdy ich dane są przetwarzane na terenie Unii Europejskiej, ale i w przypadku ich przekazywania do podwykonawców w państwach trzecich, przykładowo w ramach korzystania z usług chmurowych. Według badań Eurostatu przeprowadzonych w 2014 r., ponad 20% badanych[4] korzystało z usług przechowywania plików w chmurze obliczeniowej. Badania te wykazały również, że duża część ankietowanych, bo aż 26%, chociaż używała Internetu, nie potrafiła zdefiniować, czym są usługi przetwarzania w chmurze i w związku z tym wskazać, czy z nich korzysta. Z kolei ponad 40% korzystających z Internetu i świadomych istnienia usług przechowywania danych

[2] M. Rojszczak, *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 335.

[3] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy*, COM (2016) 288 final, s. 3.

[4] W przedziale wiekowym 16–74 lata.

w chmurze jako przyczynę niekorzystania z tych usług wskazało obawy związane z bezpieczeństwem lub zagrożeniem prywatności[5].

Rozważania nad zagadnieniem transferów danych mają więc bardzo praktyczny wymiar, co więcej – problematyka ta stanowi jedno z poważniejszych wyzwań pod względem regulacyjnym, a także teoretycznoprawnym we współczesnym świecie[6] i jeden z głównych obszarów, na którym widoczna jest potrzeba reform. Ostatnie zmiany wprowadzone przez RODO[7] w zakresie ochrony danych osobowych oraz ich transferu do państw trzecich stanowią temat dyskusji w literaturze przedmiotu. Wybór rozporządzenia jako metody legislacyjnej pozwolił na znaczne zbliżenie rozwiązań prawnych w państwach członkowskich Unii Europejskiej. Zgodnie z nowymi przepisami rozporządzenie obejmuje nie tylko administratorów danych, lecz także podmioty przetwarzające – procesorów danych. Podjęto również próbę uregulowania problematyki transferów dalszych, a zatem transferów danych dokonywanych przez administratora z państwa trzeciego. RODO wyraźnie dopuściło możliwość korzystania z różnego rodzaju klauzul modelowych oraz wiążących reguł korporacyjnych. Kontrowersje wśród zainteresowanych podmiotów budzi radykalna zmiana w kwestii zaostrzenia sankcji za nieprzestrzeganie przepisów. Ze względu na nieprecyzyjność rozporządzenia często spotyka się ono z głosami krytyki, pojawiła się także teza o straconej szansie[8].

Liczne komentarze wywołała również wprowadzona w 2016 roku Tarcza Prywatności, regulująca przepływ danych do Stanów Zjednoczonych, będąca niejako konsekwencją przełomowego orzeczenia Trybunału Sprawiedliwości dotyczącego sprawy Maximiliana Schremsa[9]. Niepewność prawna dodatkowo pogłębiła się w związku z ogłoszonym 16 lipca 2020 roku wyrokiem Trybunału Sprawiedliwości unieważniającym program Tarczy Prywatności[10]. Wyrok zniweczył podstawy prawne transferu danych osobowych do USA przyjęte przez organy ochrony danych w krajach UE oraz przez europejskich przedsiębiorców. Trybunał zakwestionował bowiem dokonane przez Komisję Europejską ustalenie, zgodnie z którym Stany Zjednoczone zapewniają stopień ochrony merytorycznie równoważny temu, który zagwarantowany jest przez RODO.

---

[5] P. Reinecke, H. Seybert, *Internet and cloud services – statistics on the use by individuals*, „Statistics in focus" 16/2014, *passim*.

[6] D. Karwala, *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018, s. 18.

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE. L. z 2016 r. Nr 119, s. 1 ze zm.), dalej: rozporządzenie 2016/679 lub RODO.

[8] Zob. P. Litwiński, *Transfer danych osobowych do państw trzecich w pracach nad ogólnym rozporządzeniem o ochronie danych – stracona szansa* [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 303.

[9] Wyrok Trybunału Sprawiedliwości z 6.10.2015 r., C-362/14, ECLI: EU:C:2015:650.

[10] Wyrok Trybunału Sprawiedliwości z 16.7.2020 r., C-311/18, ECLI:EU:C:2020:559.

2. Dyrektywa 95/46 i potrzeba reform

W zakresie regulacji unijnych dotyczących przekazywania danych osobowych do państw trzecich warto pod rozwagę wziąć dwa akty prawne – poprzednio obowiązującą i nieaktualną już dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[11] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, obowiązujące aktualnie od maja 2018 r, zwane również RODO.

Cele i wartości będące fundamentem wprowadzonego w 2016 roku rozporządzenia pozostają takie same, jak te będące podstawą rozwiązań przyjętych w dyrektywie 95/46. Zgodnie z motywem 101 preambuły do rozporządzenia: „przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy (…) obniżać stopnia ochrony osób fizycznych zapewnianego w Unii niniejszym rozporządzeniem, także w przypadkach dalszego przekazywania danych osobowych". W motywie 6 prawodawca unijny podkreślił znaczenie operacji przekazywania danych w kontekście rozwoju handlu i współpracy międzynarodowej, wskazując, iż: „Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych".

Przed wejściem w życie rozporządzenia 2016/679 niezadowolenie z regulacji prawnej widoczne było wśród przedsiębiorców, organów nadzorczych, organów administracji krajowej oraz unijnej, a wreszcie wśród samych obywateli UE. Kontrowersje budziły przede wszystkim istotne różnice w podejściu administratorów danych. Niektóre organizacje przeznaczały ogromne środki w celu zapewnienia zgodności z obowiązującym prawem, podczas gdy inne zupełnie nie spełniały stawianych wymogów. Na szerokie rozbieżności pomiędzy regulacjami poszczególnych państw członkowskich wskazywano już we wnioskach z pierwszego raportu z wykonania dyrektywy 95/46[12]. Brak harmonizacji rozwiązań na obszarze UE skutkował pojawieniem się niekorzystnego zjawiska zwanego *forum shopping,* czyli poszukiwania wśród państw członkowskich najkorzystniejszej sytuacji prawnej w zależności od tego, jak interpretowane były przepisy dotyczące ochrony danych osobowych[13]. Komisja Europejska wskazywała, iż: „nazbyt liberalne podejście w niektórych państwach członkowskich – oprócz tego, że jest sprzeczne z dyrektywą – zagraża osłabieniem ochrony w całej UE,

[11] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE. L. z 1995 r. Nr 281, s. 31 ze zm.), dalej: dyrektywa 95/46.

[12] Komisja Europejska, *Report from the Commission, First report on the implementation of the Data Protection Directive (95/46/EC)*, 15.5.2003 r., COM(2003) 265 final, p. 18.

[13] Grupa Robocza Art. 29, *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46 z 24.10.1995 r.*, 25.11.2005 r., 2093–01/05/PL, WP 114, s. 3.

ponieważ w warunkach gwarantowanego dyrektywą swobodnego przepływu danych może doprowadzić do przechodzenia na «najmniej uciążliwe» kanały przesyłowe”[14]. W literaturze podkreślano, że przyczyną problemu była już sama regulacja artykułu 26 ust. 2 dyrektywy 95/46, gdyż pozostawiała: „nadmierną swobodę w zakresie uregulowania w prawodawstwach krajowych szczegółowych zasad transgranicznego transferu danych osobowych, niwecząc plan wypracowania jednolitego systemu eksportu danych poza EOG”[15].

Krytykowano również regulację dotyczącą przeprowadzania przez Komisję Europejską oceny adekwatności państw trzecich. Procedura była skomplikowana, co więcej, nie istniały jednoznaczne przesłanki takiej oceny. Odczuwalny był także brak wyraźnego wskazania, że ocena może odnosić się tylko do określonych sektorów gospodarki, a nie państw jako całości. W efekcie Komisja wydała niewielką liczbę decyzji, a instytucja ta miała ograniczone znaczenie w praktyce[16]. Ponadto w niektórych państwach członkowskich istniał obowiązek występowania do organów nadzorczych o zatwierdzenie operacji transferowych opartych na decyzjach Komisji w sprawie adekwatności oraz decyzjach zatwierdzających modelowe klauzule umowne. Pojawiły się również trudności w zakresie odróżnienia operacji transferu danych od operacji tranzytu danych, co wynikało z braku precyzyjnej definicji[17]. Pomimo uchylenia dyrektywy 95/46 odpowiednie jej przedstawienie umożliwia ukazanie kierunku, w którym ewoluuje prawo unijne.

3. Rozporządzenie 2016/679 – wybrane zmiany

Wybór rozporządzenia jako metody legislacyjnej, którą posłużył się unijny prawodawca, pozwolił na znaczne zbliżenie rozwiązań prawnych w państwach członkowskich poprzez wprowadzenie ujednoliconych przepisów, co zwiększyło pewność prawną oraz ochronę praw podstawowych osób fizycznych. Problematyka transferu danych do państw trzecich lub organizacji międzynarodowych uregulowana została w rozdziale V RODO.

Na wstępie należy wskazać, iż rozporządzenie 2016/679 nadal nie wprowadziło precyzyjnej definicji pojęcia przekazywania (transferu) danych osobowych, co rodzi szereg wątpliwości. Problem podkreślał m.in. Europejski Inspektor Ochrony Danych. Jak wskazywał w swojej opinii: „Określenie czym jest transfer, a czym nie jest, powinno zostać w sposób wyraźny zaadresowane w projekcie, w szczególności w odniesieniu do sieci informatycznych, gdzie różnica pomiędzy aktywnym transferowaniem a udostępnianiem danych ma olbrzymie znaczenie dla administratorów oraz jednostek,

[14] Komisja Europejska, *Report*…, p. 19.

[15] B. Marcinkowski, *Kontrola transgranicznego transferu danych osobowych* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009, s. 279.

[16] D. Karwala, *Komercyjne*…, s. 320.

[17] D. Karwala, *Komercyjne*…, s. 320.

w szczególności w kontekście rozstrzygnięcia zagadnień prawa właściwego”[18]. RODO nie rozwiązało problemów definicyjnych, co wywołuje głosy krytyki.

Podobnie jak dyrektywa 95/46, rozporządzenie 2016/679 jako regułę wprowadza zakaz transferu danych osobowych do państw trzecich oraz organizacji międzynarodowych. Zakaz ten nie jest wyrażony wprost w przepisach rozporządzenia, jednak należy wyprowadzić go z całokształtu regulacji. Może on zostać uchylony wyłącznie po ustaleniu, iż państwo trzecie zapewnia adekwatny poziom ochrony lub eksporter danych spełnia inne przesłanki określone w rozdziale V RODO.

Interesującą zmianą dokonaną w ramach unijnej regulacji stanowi objęcie nią nie tylko administratorów danych, lecz także podmiotów przetwarzających (procesorów danych), co jest reakcją na rozwój pewnych zjawisk, w szczególności usługi *cloud computing*. Już art. 44 rozporządzenia obok administratorów danych uwzględnia także procesorów danych. Przekazanie danych osobowych dokonane przez unijne podmioty przetwarzające warto poddać bardziej szczegółowej analizie. Jak wskazuje L. Moerel, wymogi w zakresie transferu danych powinny dotyczyć takich podmiotów wyłącznie, gdy przekazują dane dalszym podmiotom przetwarzającym z państw trzecich [*processor-to-(sub)processor transfers*] i tylko w zakresie ich „własnych” obowiązków[19]. Autorka podnosi, iż reżim rozdziału V RODO nie powinien być stosowany w stosunku do unijnego procesora, gdy transferuje on zwrotnie dane do administratora danych z państwa trzeciego (który korzysta z usług procesora), jak również, gdy przekazuje on dane do innego administratora z państwa trzeciego. W tym kontekście określić należy bowiem status podmiotów przetwarzających. Jak wskazuje Grupa Robocza Art. 29: „Przetwarzający działa «w imieniu administratora danych». Działanie w czyimś imieniu oznacza działanie w interesie innego podmiotu i przypomina pojęcie prawne «przekazania uprawnień». W przepisach dotyczących ochrony danych wzywa się przetwarzającego do wykonania instrukcji wydanych przez administratora danych, przynajmniej w odniesieniu do celu przetwarzania oraz istotnych elementów lub środków”[20]. Warto dodatkowo podkreślić, że posługując się pojęciem transferu realizowanego przez procesora danych, uwzględnić można jedynie faktyczny jego wymiar. W znaczeniu prawnym przekazanie danych dokonywane jest bowiem przez administratora, ponieważ to on decyduje o przeprowadzeniu tej operacji. Jedyny wyjątek wyrażony został w art. 28 ust. 3 lit. a RODO, z którego wynika, iż podmiot przetwarzający może bez zgody administratora danych przekazać je do państwa trzeciego w sytuacji, gdy taki obowiązek wynika z prawa UE lub prawa państwa członkowskiego, któremu podlega procesor danych. Pomimo tego, że podmiot przetwarzający dokonuje w tej sytuacji przekazania danych bez polecenia administratora lub nawet bez jego wiedzy, zgodnie z brzmieniem powołanego przepisu nadal występować będzie w roli podmiotu prze-

[18] Europejski Inspektor Ochrony Danych, *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7.3.2012 r., pkt 108, p. 18–19.

[19] L. Moerel, *GDPR conundrums: Data transfers*, „Privacy Tracker”, 9.6.2016 r., <https://iapp.org/news/a/gdpr-conundrums-data-transfer/>, [dostęp: 24.7.2020 r.].

[20] Grupa Robocza Art. 29, *Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”*, 16.2.2010 r., 00264/10/PL, WP 169, s. 28.

twarzającego. Warto zaznaczyć, iż ze względu na status procesora danych, który nie realizuje swych własnych interesów, lecz wypełnia polecenia administratora, wykluczyć należy możliwość powoływania się przez podmiot przetwarzający na odstępstwa uwzględnione w art. 49 rozporządzenia, które umożliwiają transfer danych osobowych w razie braku decyzji stwierdzającej odpowiedni stopień ochrony (art. 45 ust. 3 RODO) lub braku odpowiednich zabezpieczeń (art. 46 RODO), w tym wiążących reguł korporacyjnych (art. 47 RODO)[21].

Omawiając najciekawsze zmiany wprowadzone przez RODO, nie sposób pominąć problematyki dalszych transferów danych, a zatem transferów danych dokonywanych przez administratora z państwa trzeciego. Operacje takie na obecnym etapie rozwoju gospodarczego i technologicznego stały się powszechnym zjawiskiem. W świetle art. 44 rozporządzenia wydaje się, iż celem unijnego prawodawcy było poddanie procesu dalszego przekazania danych takim samym wymogom, jak te dotyczące „pierwotnego" transferu, który realizowany jest przez eksportera unijnego. Takie uregulowanie kwestii dalszego przekazywania danych może budzić kontrowersje.

Aby zapewnić zgodność z prawem unijnym w przypadku dalszego przekazania danych konieczna jest realizacja wymogów określonych w RODO przez administratora z państwa trzeciego – co rodzi poważne wątpliwości, gdyż przepisów rozporządzenia 2016/679 nie stosuje się zasadniczo w stosunku do podmiotów z państw trzecich. W alternatywnej wersji konieczna byłaby realizacja przedmiotowych obowiązków przez administratora z państwa członkowskiego. Nałożenie ich na unijnego eksportera danych powinno odbywać w warunkach prawnie określonych, z zapewnieniem po jego stronie stosownej wiedzy w kwestii planowanego przez importera danych dalszego ich przekazania. Jednakże, gdy transfer realizowany jest do importerów z tych państw trzecich, w stosunku do których Komisja wydała decyzję stwierdzającą adekwatny poziom ochrony, pojawia się wątpliwość, czy wystarczające jest, aby odbiorca danych z „adekwatnego" państwa trzeciego stosował przepisy prawa, któremu podlega, w celu zapewnienia legalności operacji dalszego przekazania danych. W tym kontekście uwzględnić należy brzmienie art. 45 ust. 2 lit. a rozporządzenia 2016/679, który wśród elementów, jakie powinny być brane pod uwagę w ramach oceny adekwatności, wymienia: „zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej". Założeniem jest zatem obowiązywanie w „adekwatnym" państwie trzecim regulacji, która zapewnienia odpowiednią ochronę danych osobowych podczas dalszego ich przekazywania.

Kolejną zmianą wprowadzoną rozporządzeniem, która dla praktyki obrotu może mieć istotne znaczenie, jest wyraźne dopuszczenie korzystania z różnego rodzaju klauzul modelowych. Ponadto w przepisach uznano instrument w postaci wiążących reguł korporacyjnych, które będą mogły być stosowane także przez podmioty przetwarzające dane na zlecenie[22]. Wprowadzono nowe gwarancje ochrony w postaci „zatwierdzonego

[21] D. Karwala, *Komercyjne*…, s. 396.

[22] D. Karwala, *Komercyjne*…, s. 447–448.

kodeksu postępowania" (art. 46 ust. 2 lit. e RODO) oraz „zatwierdzonego mechanizmu certyfikacji" (art. 46 ust. 2 lit. f RODO). Nowością jest wyraźne wymienienie instrumentów służących do wymiany danych osobowych pomiędzy organami lub podmiotami publicznymi (art. 46 ust. 2 lit. a RODO, art. 46 ust. 3 lit. b RODO)[23]. Jak wskazuje D. Karwala:

> w dalszym ciągu instrumenty transferowe, jakimi mogą dysponować zainteresowane podmioty, wymagają określonej ingerencji „urzędowej". Może ona przybrać formę zatwierdzenia (np. wiążących reguł korporacyjnych) bądź autoryzacji krajowej (zezwolenia na przeprowadzenie operacji transferu danych z wykorzystaniem określonego instrumentu). Podstawowa różnica w stosunku do dotychczasowego stanu prawnego wiąże się tym samym z ograniczeniem sytuacji, gdy dochodziło do dublowania się tego rodzaju zatwierdzeń oraz autoryzacji, na co zwracano uwagę przede wszystkim w związku z korzystaniem z wiążących reguł korporacyjnych[24].

Gdy transfer danych ma zostać zrealizowany do państwa trzeciego, w stosunku do którego nie wydano decyzji o odpowiedniości ochrony i nie jest on oparty na odpowiednich gwarancjach, może odbyć się na podstawie jednego z wyjątków wymienionych w art. 49 RODO. Określone w przepisie wyjątki są w dużej części zbieżne z tymi funkcjonującymi na gruncie dyrektywy 95/46. Za istotną zmianę należy jednak uznać wprowadzenie wymogu poinformowania podmiotu danych o ewentualnych zagrożeniach, z którymi – ze względu na brak decyzji Komisji oraz na brak odpowiednich gwarancji – może się dla niego wiązać taki transfer danych. Co ważne, postawiono przy tym wymóg wyraźniej zgody podmiotu danych, co wpisuje się w koncepcję „poinformowanej zgody", która od dłuższego czasu postulowana była przez Grupę Roboczą art. 29. Warto zwrócić uwagę także na zupełnie nowy wyjątek, wprowadzony w art. 49 ust. 1 RODO, akapit drugi. Prawodawca unijny poprzez ten przepis zezwolił na transfer danych w interesie administratora danych (eksportera), który nie może oprzeć się na innych podstawach umożliwiających przekazanie tych danych. W takim przypadku może on dokonać transferu przy zastrzeżeniu spełnienia dodatkowych przesłanek: transfer nie może być powtarzalny, powinien dotyczyć tylko ograniczonej liczby podmiotów i być realizowany z uwagi na ważne uzasadnione interesy realizowane przed administratora danych, wobec którego nie mają charakteru nadrzędnego interesy ani prawa podmiotu danych. Administrator powinien dodatkowo ocenić wszystkie okoliczności przekazu danych, a także poinformować o tym transferze krajowy organ ds. ochrony danych osobowych, jak również podmiot danych. Wykładnia przepisu rodzi wątpliwości, wskutek nieprecyzyjnego sformułowania o „niepowtarzalności" transferu czy ograniczonej liczbie podmiotów. Jak wskazuje X. Konarski: „Nie jest również jasne, jakie interesy eksportera danych zostaną uznane za ważne i uzasadnione, tym bardziej, że w motywie 113 ogólnego rozporządzenia wskazano

[23] X. Konarski, *Transfer danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych a dotychczasowy stan prawny w UE i w Polsce* [w:] *Polska i europejska reforma ochrony danych osobowych,* red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016, s. 287.

[24] D. Karwala, *Komercyjne*…, s. 449.

cele badań naukowych i historycznych oraz cele statystyczne, nie doprecyzowując, czy te właśnie cele są uzasadnione w rozumieniu art. 49 ust. 1, akapit drugi i czy inne jeszcze za takie mogą zostać uznane (np. cele związane z działalnością gospodarczą eksportera danych)"[25].

Przepisy rozporządzenia wprowadzają radykalną zmianę w kwestii sankcji za nieprzestrzeganie regulacji. Wysokość i dolegliwość kar znacznie wzrosła. Zgodnie z art. 83 ust. 5 lit. c RODO naruszenie przepisów o transferze danych podlega grzywnie administracyjnej sięgającej aż 20 000 000 euro, a w przypadku przedsiębiorstwa – sięgającej 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Przed wejściem w życie rozporządzenia dobór sankcji pozostawiono ustawodawstwom krajowym. W większości przypadków były to sankcje karne lub administracyjne, przewidujące kary pieniężne, które nie przekraczały kwoty kilkudziesięciu tysięcy euro[26]. Zmiana ma mobilizować przedsiębiorców oraz podmioty sektora publicznego do większej staranności w zakresie ochrony danych osobowych osób fizycznych.

4. Wyrok w sprawie M. Schrems i jego wpływ na regulację unijną

Omawiając najnowsze zmiany w zakresie zasad bezpiecznego transferu danych osobowych do państw trzecich, nie sposób pominąć dwóch zdarzeń – afery wywołanej przez Edwarda Snowdena oraz będącego jej konsekwencją precedensowego wyroku Trybunału Sprawiedliwości w sprawie Maximilian Schrems przeciwko *Data Protection Commissioner*. Wyrok TSUE wywarł bowiem ogromny wpływ na interpretację przepisów rozdziału V rozporządzenia 2016/679. Jak wskazuje się w doktrynie: „rewelacje [E. Snowdena – M.G.] stanowiły jeden z głównych katalizatorów unijnej reformy w zakresie danych osobowych"[27].

W połowie 2013 roku Edward Snowden – były pracownik amerykańskiej Agencji Bezpieczeństwa Krajowego (ang. *National Security Agency, NSA*) – opublikował tajne dokumenty amerykańskich służb wywiadowczych. Ujawnione materiały wskazywały na kontrowersyjne praktyki służb, polegające w szczególności na uzyskiwaniu dostępu do danych osobowych, przetwarzanych i przesyłanych w sieci Internet w ramach usług wiodących dostawców, takich jak Google, Microsoft, Yahoo!, Facebook, Apple czy LinkedIn. Wiadomość ta zbulwersowała opinię publiczną w Europie oraz w USA i ujawniła poważny problem inwigilacji w Internecie. Nadto pojawiła się dyskusja wokół obowiązującego wówczas programu Bezpiecznej Przystani. Bezpieczna Przystań (ang. *Safe Harbour*) była programem zatwierdzonym decyzją Komisji Europejskiej[28],

[25] X. Konarski, *Transfer*…, s. 290.

[26] X. Konarski, *Transfer*…, s. 292.

[27] J. Kulesza, *USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining?*, „Groningen Journal of International Law" 2014/2(2), p. 85, <https://grojil.files.wordpress.com/2015/04/grojil_volume-2_issue-2.pdf>, [dostęp: 26.6.2020 r.].

[28] Decyzja Komisji 2000/520/WE z 26.7.2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności

mającym zapewnić odpowiednią ochronę danych osobowych przekazywanych przed podmiot z UE do przedsiębiorstwa z siedzibą w Stanach Zjednoczonych. Większość z pojawiających się w dokumentach podmiotów z sektora prywatnego należała do tego programu.

Dyskusja, którą wywołały informacje ujawnione przez Snowdena, skłoniła studenta prawa Maximiliana Schremsa do wniesienia skargi do irlandzkiego organu ds. ochrony danych (*Data Protection Commissioner*). Schrems podniósł, iż prawo i praktyka Stanów Zjednoczonych nie zapewniają rzeczywistej ochrony danych osobowych przekazywanych do tego państwa z obszaru UE, w tym w szczególności ochrony użytkowników serwisu Facebook. Dane z serwisu są bowiem przekazywane przez irlandzką spółkę (Facebook Ireland Ltd) na serwery znajdujące się na terytorium USA, należące do spółki Facebook Inc. Prawo USA pozwalało na gromadzenie danych osobowych obywateli UE, którzy nie mieli zapewnionej skutecznej ochrony prawnej.

W toku postępowania pojawiły się wątpliwości, czy krajowy organ nadzorczy może zablokować taką operację przekazywania danych. W kwestii tej wypowiedział się m.in. Rzecznik Generalny Y. Bot, który uznał, iż: „biorąc pod uwagę istotną rolę krajowych organów nadzorczych w zakresie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych, ich uprawnienia interwencyjne powinny pozostać nieograniczone, nawet jeśli Komisja przyjęła decyzję na podstawie art. 25 ust. 6 dyrektywy 95/46”[29]. Ponadto Rzecznik wskazał, iż organy krajowe mają prawo do: „wyrobienia sobie własnej opinii co do ogólnego poziomu ochrony zapewnianego przez państwo trzecie”[30], a „ze względu na opisane (…) naruszenia praw podstawowych nie można uznać, że wprowadzony przez nią [przez decyzję 2000/520/WE – M.G.] system Bezpiecznej Przystani zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do Stanów Zjednoczonych w ramach tego systemu”[31].

Wyrok w sprawie zapadł 6.10.2015 roku[32]. Rozstrzygając spór, Trybunał Sprawiedliwości uznał, iż decyzja Komisji w sprawie adekwatności państwa trzeciego nie może wpływać na osłabienie uprawnień krajowych organów nadzorczych do rozpatrzenia skargi obywatela, który zarzuca, że państwo to nie zapewnia ochrony danych na gruncie prawa wewnętrznego. Krajowy organ nadzorczy nie powinien być zatem bezwzględnie związany ustaleniami w zakresie adekwatności zawartymi w decyzji Komisji. Co więcej, Trybunał dokonał oceny decyzji 2000/520/WE dotyczącej programu Bezpiecznej Przystani i doszedł do wniosku, że program ten nie spełnia wymogów

w ramach „bezpiecznej przystani” oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz. Urz. WE. L. z 2000 r. Nr 215, s. 7 ze zm), dalej: decyzja 2000/520/WE.

[29] Opinia Rzecznika Generalnego Y. Bota z 23.9.2015 r. w sprawie M. Schrems przeciwko Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:627, pkt 71.

[30] Opinia Rzecznika Generalnego Y. Bota z 23.9.2015 r. w sprawie M. Schrems przeciwko Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:627, pkt 61.

[31] Opinia Rzecznika Generalnego Y. Bota z 23.9.2015 r. w sprawie M. Schrems przeciwko Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:627, pkt 216.

[32] Wyrok Trybunału Sprawiedliwości z 6.10.2015 r., C-362/14, ECLI: EU:C:2015:650.

wynikających z prawa unijnego. Uregulowanie umożliwiające organom publicznym uzyskanie „powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego”[33]. Decyzji zatwierdzającej program Bezpiecznej Przystani w szczególności zarzucono, iż: „zasady te mają (…) zastosowanie wyłącznie do organizacji amerykańskich, które dokonały samocertyfikacji, otrzymujących dane osobowe z Unii, przy czym nie wymaga się, aby władze publiczne Stanów Zjednoczonych zostały zobowiązane do poszanowania tych zasad”[34]. Pierwszeństwo nad zasadami programu Bezpiecznej Przystani miały bowiem przepisy Stanów Zjednoczonych, m.in. dotyczące bezpieczeństwa państwowego i interesu publicznego, co umożliwiało władzom publicznym istotną ingerencję w dane osobowe obywateli UE. Prawo, które nie przewidywało rozwiązań w celu zapewnienia jednostce dostępu do zebranych na jej temat danych, ich zmiany lub usunięcia, należało ocenić jako naruszające podstawowe prawa jednostki.

Uznanie decyzji za nieważną zniweczyło podstawy prawne transferu danych osobowych do USA przyjęte przez organy ochrony danych w krajach UE oraz przez tysiące europejskich przedsiębiorców. Omawiany wyrok wywołał duże poruszenie wśród zainteresowanych podmiotów. Komisja rozpoczęła prace nad nowymi rozwiązaniami, które ostatecznie przybrały kształt Tarczy Prywatności. Jak wskazuje się w literaturze: „wyrok (…) podważył logiczną spójność pozostałych podstaw prawnych transferu danych, poza samą Bezpieczną Przystanią”[35]. W rozstrzygnięciu Trybunał wskazał, że: „operacja przekazywania danych osobowych z państwa członkowskiego do państwa trzeciego polega sama w sobie na przetwarzaniu danych osobowych w rozumieniu art. 2 lit. b dyrektywy 95/46 (…) dokonywanym na terytorium państwa członkowskiego”[36]. W rezultacie operacje transferowe oraz przepisy je regulujące należy oceniać w świetle unijnej regulacji dotyczącej praw podstawowych. Interpretacja Trybunału odcisnęła piętno na ostatecznym kształcie rozdziału V rozporządzenia 2016/679. Podniesione zostały oczekiwania względem państw trzecich, zastąpiono wymóg „adekwatnej” ochrony standardem „zasadniczej równoważności”. Można przypuszczać, iż w związku z tym decyzje Komisji w sprawie adekwatności staną się jeszcze trudniejsze do wypracowania[37]. Odnoszenie wygórowanych oczekiwań wobec państw trzecich, które nie mają silnych tradycji demokratycznych (np. do państw Bliskiego Wschodu czy też państw afrykańskich), może prowadzić do tego, że w stosunku do większości państw trzecich przyjęcie decyzji o adekwatności nigdy nie nastąpi. Następstwem omawianego wyroku jest zatem o wiele mniejszy poziom „otwartości” regulacji unijnej na rozwiązania funkcjonujące w państwach trzecich. Kontrowersje budzi także podkreślenie przez Trybunał

[33] Wyrok Trybunału Sprawiedliwości z 6.10.2015 r., C-362/14, ECLI: EU:C:2015:650, pkt 94.

[34] Wyrok Trybunału Sprawiedliwości z 6.10.2015 r., C-362/14, ECLI: EU:C:2015:650, pkt 82.

[35] C. Kuner, *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, „Legal Studies Research Paper Studies” 2016/14, p. 1.

[36] Wyrok Trybunału Sprawiedliwości z 6.10.2015 r., C-362/14, ECLI: EU:C:2015:650, pkt 44.

[37] D. Karwala, *Komercyjne*…, s. 430.

Sprawiedliwości roli krajowych organów nadzorczych kosztem Komisji. W opinii C. Kunera może to prowadzić do: „powstania mozaiki odmiennych ocen pomiędzy organami nadzorczymi oraz sądami państw członkowskich dotyczących poziomu ochrony w państwach trzecich, co z kolei może prowadzić do nierównomiernej ochrony jednostek w ramach UE”[38]. W świetle art. 58 ust. 2 lit. j RODO każdy organ krajowy ma możliwość zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej. Taka regulacja stwarza zatem ryzyko niejednolitego stosowania decyzji Komisji w sprawie adekwatności[39].

W konsekwencji do omawianego wyroku Grupa Robocza Art. 29, opiniując m.in. projekt decyzji Komisji 2016/2295[40] w sprawie odpowiedniej ochrony danych osobowych przez niektóre państwa, wskazała, iż przed podjęciem decyzji w sprawie adekwatności powinna zostać dokonana szczegółowa analiza warunków, w których służby z państw trzecich mogą uzyskać dostęp do przekazywanych danych. Przykładowo należy zwrócić uwagę na fakt, iż, państwa takie, jak Nowa Zelandia czy Kanada, które są objęte decyzjami Komisji, należą do tzw. Sojuszu Pięciorga Oczu (ang. *Five Eyes Agreement*), czyli porozumienia instytucji szpiegowskich pomiędzy agencjami amerykańską, brytyjską, kanadyjską, australijską oraz nowozelandzką, dotyczącego przekazywania danych wywiadowczych. Pojawia się zatem wątpliwość, czy państwa takie zapewniają poziom ochrony, który jest „zasadniczo równoważny” temu obowiązującemu w UE. Dodatkowo wiele państw trzecich, dotychczas niepoddanych ocenie przez Komisję, wyłącza działalność swych agencji wywiadowczych spod ogólnej regulacji dotyczącej ochrony danych osobowych i nie uwzględnia stawianych przez Trybunał wymogów związanych z zapewnieniem nadzoru nad tego rodzaju operacjami. Okoliczności te mogą ostatecznie wpływać na osłabienie znaczenia decyzji Komisji w sprawie adekwatności.

Na zakończenie warto wskazać, iż argumenty użyte przez Trybunał wpływają także na inne mechanizmy transferowe, w szczególności na umowy transferowe czy wiążące reguły korporacyjne. Nie ulega bowiem wątpliwości, że te instrumenty, mające charakter prywatnoprawny i wiążące jedynie określone podmioty (np. strony umowy, członków korporacji), nie są w stanie przeciwdziałać praktykom organów publicznych, w szczególności służb specjalnych z państw trzecich.

5. Przepływ danych do Stanów Zjednoczonych – Tarcza prywatności

Tarcza chroniąca prywatność (ang. *Privacy Shield*) to system wspierający przepływ danych pomiędzy Unią Europejską a Stanami Zjednoczonymi. Mechanizm ten

[38] C. Kuner, *Reality*…, p. 12.

[39] C. Kuner, *Reality*…, p. 12.

[40] Decyzja wykonawcza Komisji (UE) 2016/2295 z 16.12.2016 r. zmieniająca decyzje 2000/518/WE, 2002/2/WE, 2003/490/WE, 2003/821/WE, 2004/411/WE, 2008/393/WE, 2010/146/UE, 2010/625/UE, 2011/61/UE oraz decyzje wykonawcze 2012/484/UE i 2013/65/UE w sprawie odpowiedniej ochrony danych osobowych przez niektóre państwa, na podstawie art. 25 ust. 6 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (Dz. Urz. UE. L. z 2016 r. Nr. 344, s. 83 ze zm.).

w 2016 roku zastąpił program Bezpiecznej Przystani, w reakcji na orzeczenie Trybunału Sprawiedliwości w sprawie M. Schrems. Miał na celu zapewnienie odpowiedniego poziomu ochrony danych osobowych przekazywanych od podmiotów z UE do podmiotów z siedzibą w Stanach Zjednoczonych.

Z perspektywy osoby, której dane są przetwarzane, Tarcza gwarantowała szereg korzyści, takich jak prawo do otrzymania informacji o przekazaniu danych i prawo dostępu do danych. Ponadto program pozwolił w łatwy sposób kontrolować, czy dane przedsiębiorstwo posiada certyfikat. Organizacja stosująca zasady Tarczy Prywatności zobligowana została do poinformowania podmiotu, którego dane przetwarza, jakie jest uzasadnienie tego przetwarzania i jakiego rodzaju są to dane. Podkreślano, iż przedsiębiorstwo może otrzymywać i przetwarzać dane osobowe wyłącznie w zakresie, w jakim są one istotne w świetle celu przetwarzania i musi dopilnować, by dane były ścisłe, wiarygodne, kompletne i aktualne. Decyzja o przystąpieniu do projektu należała wyłącznie do zainteresowanej organizacji i była dobrowolna. Przedsiębiorstwa amerykańskie pragnące dokonać samocertyfikacji i korzystać z przywilejów wynikających z członkostwa w programie musiały spełnić szereg wymogów – przykładowo podlegać „uprawnieniom dochodzeniowym i wykonawczym" Federalnej Komisji Handlu, Departamentu Transportu USA lub „innemu organowi ustawowemu, który skutecznie zapewni przestrzeganie zasad"[41]. Poza obowiązkiem pełnego wdrożenia wymogów Tarcza wymagała opublikowania przez organizację jej polityki prywatności[42].

Znaczny fragment preambuły do decyzji Komisji 2016/1250[43] zatwierdzającej program poświęcono analizie ustawodawstwa amerykańskiego w kwestii dostępu amerykańskich organów publicznych do danych osobowych przekazywanych z obszaru UE, w szczególności służb wywiadowczych. W motywie 88 wskazano, iż: „w Stanach Zjednoczonych wdrożono przepisy służące ograniczeniu wszelkiej ingerencji do celów bezpieczeństwa narodowego w prawa podstawowe osób, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE-USA, do tego, co jest ściśle niezbędne, aby osiągnąć uzasadniony cel". Zgodnie z motywem 123: „Stany Zjednoczone zapewniają skuteczną ochronę prawną przed ingerencją swoich organów wywiadowczych w prawa podstawowe osób, których dane są przekazywane z Unii do Stanów Zjednoczonych w ramach Tarczy Prywatności UE-USA". Można przypuszczać, że wszelkie te zapewnienia były reakcją na rozstrzygnięcie Trybunału Sprawiedliwości w sprawie M. Schrems. Pomimo tego w literaturze przedmiotu nadal wyrażane były liczne obawy. Jak zauważa D. Karwala:

[41] Załącznik II do Decyzji wykonawczej Komisji 2016/1250 z 12.7.2016 r. przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA (Dz. Urz. UE. L. z 2016 r. Nr 207, s. 1 ze zm).

[42] D. Karwala, *Komercyjne*…, s. 437.

[43] Decyzja wykonawcza Komisji (UE) 2016/1250 z 12.7.2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA (Dz. Urz. UE. L. z 2016 r. Nr 207, s. 1 ze zm.).

> Ochrona (…) nie może być (…) w pełni skuteczna, jeśli uwzględni się specyfikę przedmiotowego programu, przeznaczonego dla biznesowych (komercyjnych) operacji transferowych. Ze swej istoty mechanizm ten nie będzie gwarantował pełnej ochrony danych przekazywanych do Stanów Zjednoczonych w sferze, która związana jest z bezpieczeństwem narodowym czy działalnością amerykańskich organów ścigania. Nie znaczy to jednak, iż w sposób pośredni nie oddziałuje on również na ten obszar. Wpływ ten jest co prawda wyraźnie widoczny, do czasu jednak wprowadzenia przez stronę amerykańską dodatkowych rozwiązań, wzorowanych na tych funkcjonujących w UE (co jednak odbywa się w oderwaniu od funkcjonowania samego programu, choć ma z nim związek), zastrzeżenia kierowane wobec programu Tarcza Prywatności (a pośrednio – do amerykańskich służb wywiadowczych i organów ścigania) będą nadal zgłaszane[44].

Pojawiły się także pytania o zgodność Tarczy z prawem unijnym, w tym z Kartą praw podstawowych. Mimo wprowadzonych nowych rozwiązań, nadal istniała wątpliwość, czy program gwarantuje pełną ochronę danych osobowych w sferze związanej z działalnością amerykańskich organów ścigania.

W ramach sporu, jaki zaistniał pomiędzy *Data Protection Commissioner* a *Facebook Ireland Ltd* i Maximillianem Schremsem w dniu 9 maja 2018 r. do Trybunału Sprawiedliwości wpłynął wniosek o wydanie orzeczenia w trybie prejudycjalnym. Wniosek dotyczył dokonania wykładni i zbadania ważności decyzji Komisji 2010/87/UE[45] z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych oraz decyzji wykonawczej Komisji (UE) 2016/1250 w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA. W zapadłym 16 lipca 2020 roku wyroku[46] Trybunał zakwestionował dokonane przez Komisję ustalenie, zgodnie z którym Stany Zjednoczone zapewniają stopień ochrony merytorycznie równoważny temu, który jest gwarantowany w Unii Europejskiej przez RODO. Jednocześnie stwierdzono nieważność decyzji w sprawie Tarczy Prywatności. Jednym z powodów wyroku jest dalszy dostęp do danych Europejczyków przez amerykańskie służby oraz brak uregulowania tej kwestii w sposób odpowiadający wymogom prawa unijnego. Od 16 lipca 2020 r. program ten nie może być zatem podstawą transferów danych do USA, a przedsiębiorstwa i inne podmioty powinny znaleźć inną podstawę transferu albo całkowicie transfer ten wstrzymać. W tym kontekście należy wskazać, że badanie decyzji komisji 2010/87/UE w sprawie standardowych klauzul umownych nie doprowadziło do ustaleń, które mogłoby mieć wpływ na ważność tej decyzji. Warto jednak zaznaczyć, iż podmioty nie powinny przekazywać danych do państwa, które nie zapewnia odpowiedniego poziomu ich ochrony. Administrator mający siedzibę w UE, przed dokonaniem transferu ma obowiązek sprawdzenia, czy w danym państwie stopień ochrony danych osobowych jest równoważny temu, który wymagany jest przez prawo Unii. Oznacza to konieczność

[44] D. Karwala, *Komercyjne*…, s. 443.

[45] Decyzja Komisji 2010/87/UE z 5.2.2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (Dz. Urz. UE. L. z 2010 r. Nr 39, s. 5 ze zm), zwana dalej: decyzją 2010/87/UE.

[46] Wyrok Trybunału Sprawiedliwości z 16.7.2020 r., C-311/18, ECLI:EU:C:2020:559.

dokonania przez administratorów indywidualnej oceny, która musi uwzględniać również przepisy prawa obowiązującego w państwie trzecim, w szczególności odnoszące się do dostępu organów władzy publicznej do przekazywanych danych. Wnikliwa analiza wyroku prowadzi zatem do wniosku, że w przypadku USA przedsiębiorcy i inne podmioty nie będą mogły oprzeć transferu danych na standardowych klauzulach umownych. Wyrok Trybunału wywołał poruszenie wśród zainteresowanych – orzeczenie budzi kontrowersje i pogłębia niepewność prawną.

6. Konkluzje

W dobie „eksplozji informacyjnej", z jaką mamy do czynienia we współczesnym świecie, problematyka transferów danych osobowych stanowi poważne wyzwanie, z którym musi mierzyć się unijny prawodawca. Jak słusznie wskazuje C. Kuner: „W świecie znaczonym różnorodnością rozwiązań konstytucyjnych oraz cechującym się prawnym pluralizmem iluzją jest oczekiwanie, że porządek prawny jest w stanie zapewnić ochronę jednostek w skali globalnej, poprzez przekonanie innych państw, aby te przyjęły swe własne standardy; potrzeba raczej kreatywnych rozwiązań, które uwzględniają odmienności innych systemów prawnych, oraz – docelowo – międzynarodowe rozwiązania w postaci traktatu"[47].

Należy pamiętać, że wszystkie podmioty uczestniczące w przetwarzaniu danych, również te z państw trzecich, funkcjonują w określonej przestrzeni prawnej, a przepisy o ochronie danych osobowych wprowadzane są także poza Unią. Trudno założyć, że w przypadku kolizji norm przedsiębiorca odrzuci przepisy prawa krajowego – którym wprost podlega – i zacznie stosować sprzeczne z nimi regulacje europejskie, wynikające ze zobowiązań umownych, które na siebie przyjął[48]. Obserwacja ta ukazuje słabość wprowadzonych w RODO czy w Tarczy Prywatności modelów ochrony danych przetwarzanych przez przedsiębiorców z państw trzecich i brak środków prawnych dyscyplinujących ich do przestrzegania prawa UE. Z tego względu prawodawca unijny zdecydował się rozszerzyć zakres stosowania przepisów poprzez obowiązkowe ich przestrzeganie we wszystkich czynnościach przetwarzania oraz uzależnić od tego możliwość przekazania danych do podmiotów z państw trzecich. Model ten wydaje się mieć w znacznym zakresie charakter deklaratywny, gdyż jest trudny do stosowania w praktyce. Orzecznictwo Trybunału Sprawiedliwości, uchylenie dyrektywy i zastąpienie jej nowym rozporządzeniem, a także decyzje podejmowane przez Komisję Europejską mają na celu uzupełnianie luk prawnych i zapewnienie jak najskuteczniejszej ochrony praw podstawowych obywateli unijnych.

Wybór rozporządzenia jako metody legislacyjnej, którą posłużył się unijny prawodawca, pozwolił na zbliżenie rozwiązań prawnych i zniweczył różnice w podejściu administratorów danych w poszczególnych państwach członkowskich. Przepisy

[47] C. Kuner, *Safe Harbor before the EU Court of Justice*, „Cambridge Journal of International and Comparative Law", 13.4.2015 r., <http://cjicl.org.uk/2015/04/13/safe-harbor-before-the-eu-court-of-justice>, [dostęp: 28.4.2018 r.].

[48] M. Rojszczak, *Ochrona...*, s. 374.

rozporządzenia wyraźnie dopuściły korzystanie z różnego rodzaju klauzul modelowych oraz wiążących reguł korporacyjnych. Dodatkowo wprowadzono nowe gwarancje ochrony w postaci zatwierdzonego kodeksu postępowania i zatwierdzonego mechanizmu certyfikacji. Jednakże objęcie rozporządzeniem procesorów danych stanowi raczej wyraz konieczności spowodowanej rozwojem pewnych zjawisk, w szczególności usługi *cloud computing*, niż przemyślany i konsekwentny zabieg. W znaczeniu prawnym przekazania danych dokonuje bowiem administrator danych[49]. Nałożenie wymogów wynikających z rozdziału V RODO na operacje dalszego transferu danych również budzi wątpliwość, gdyż rozszerza zakres odpowiedzialności unijnych administratorów danych w stosunku do czynności, o których decydować mogą administratorzy z państw trzecich. Problematyczne okazało się także wprowadzenie przez unijnego prawodawcę, jako wyjątku, zezwolenia na transfer danych dokonany w ważnym, prawnie uzasadnionym interesie realizowanym przez administratora.

Na skutek wyroku Trybunału Sprawiedliwości w sprawie M. Schrems od 2015 roku podniesione zostały oczekiwania względem państw trzecich, a wymóg „adekwatnej" ochrony zastąpiono standardem „zasadniczej równoważności". Decyzje Komisji w sprawie adekwatności stały się zatem jeszcze trudniejsze do wypracowania. Dodatkowo w świetle art. 58 ust. 2 lit. j RODO każdy organ krajowy może zawiesić przepływ danych do odbiorcy w państwie trzecim, co stwarza ryzyko niejednolitego stosowania decyzji Komisji w sprawie adekwatności w poszczególnych państwach członkowskich.

W zapadłym 16 lipca 2020 roku wyroku Trybunał Sprawiedliwości stwierdził nieważność decyzji w sprawie Tarczy Prywatności, wskazując, iż Stany Zjednoczone nie zapewniają stopnia ochrony merytorycznie równoważnego temu, który gwarantowany jest w Unii Europejskiej. Program ten nie może być obecnie podstawą transferów danych do USA, a administratorzy powinni znaleźć nową podstawę transferu albo całkowicie go wstrzymać. Taki stan rzeczy powoduje wzrost niepewności prawnej, co dla zainteresowanych podmiotów jest szczególnie problematyczne z uwagi na fakt, iż dolegliwość kar za nieprzestrzeganie przepisów znacznie wzrosła.

Rozwiązaniom wprowadzonym w rozdziale V RODO nie sposób przyznać miana rewolucyjnych[50]. Reformy budzą kontrowersje i spotykają się z głosami krytyki. Jak wskazuje się w literaturze:

> oceniając systemowo, podstawowe zasady przekazywania danych osobowych do państw nienależących do Europejskiego Obszaru Gospodarczego nie uległy zmianie. Uzasadnia to postawienie tezy o straconej szansie. Stracono szansę ponownego, kompleksowego uregulowania problematyki transferów danych osobowych (…). Zamiast tego mamy znane nam wszystkim od lat instytucje, które spróbowano dostosować do nowej rzeczywistości. Jednak kosmetyczny w gruncie rzeczy charakter zmian każe zadać pytanie o sens ich dokonywania"[51].

[49] D. Karwala, *Komercyjne*…s. 400.

[50] P. Litwiński, *Transfer*…, s. 303.

[51] P. Litwiński, *Transfer*…, s. 303.

Z drugiej strony wskazuje się także, iż niezasadne byłoby całkowite zerwanie (poprzez wprowadzenie oczekiwanej przez wielu „rewolucji") z dotychczasowymi mechanizmami funkcjonującymi na gruncie przepisów dyrektywy 95/46 i doświadczeniami wypracowanymi przez Grupę Roboczą Art. 29 oraz zdobytymi w praktyce obrotu, gdyż mogłoby to przynieść trudne do przewidzenia skutki[52].

Bibliografia

- Europejski Inspektor Ochrony Danych, *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7.3.2012 r.
- Grupa Robocza Art. 29, *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust.1 dyrektywy 95/46 z 24.10.1995 r.*, 25.11.2005 r., 2093–01/05/PL, WP 114.
- Grupa Robocza Art. 29, *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, 16.2.2010 r., 00264/10/PL, WP 169.
- Karwala D., *Komercyjne transfery danych osobowych do państw trzecich*, Warszawa 2018.
- Komisja Europejska, *Report from the Commission, First report on the implementation of the Data Protection Directive (95/46/EC)*, 15.5.2003 r., COM(2003) 265 final.
- Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Platformy internetowe i jednolity rynek cyfrowy. Szanse i wyzwania dla Europy*, COM (2016) 288 final.
- Konarski X., *Transfer danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych a dotychczasowy stan prawny w UE i w Polsce* [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016.
- Kulesza J., *USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining*?, „Groningen Journal of International Law" 2014/2(2).
- Kuner C., *Reality and Illusion in EU Data Transfer Regulation Post Schrems*, „Legal Studies Research Paper Studies" 2016/14.
- Kuner C., *Safe Harbor before the EU Court of Justice*, „Cambridge Journal of International and Comparative Law", 13.4.2015 r., <http://cjicl.org.uk/2015/04/13/safe-harbor-before-the-eu-court-of-justice>, [dostęp: 28.4.2018 r.].
- Litwiński P., *Transfer danych osobowych do państw trzecich w pracach nad ogólnym rozporządzeniem o ochronie danych – stracona szansa* [w:] *Polska i europejska reforma ochrony danych osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2016.
- Marcinkowski B., *Kontrola transgranicznego transferu danych osobowych* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009.
- Moerel L., *GDPR conundrums: Data transfers*, „Privacy Tracker", 9.06.2016 r., <https://iapp.org/news/a/gdpr-conundrums-data-transfer/>, [dostęp: 24.7.2020 r.].
- Opinia Rzecznika Generalnego Y. Bota z 23.9.2015 r. w sprawie M. Schrems przeciwko Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:627.
- Reinecke P., Seybert H., *Internet and cloud services – statistics on the use by individuals*, „Statistics in focus" 16/2014.
- Rojszczak M., *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

[52] D. Karwala, *Komercyjne*…, s. 445.