TRANSFORMACJE PRAWA PRYWATNEGO
1/2018 ISSN 1641–1609

MARCIN ROJSZCZAK*

SKUTECZNOŚĆ OCHRONY PRAW PODMIOTÓW DANYCH WYNIKAJĄCYCH Z PRAWA UNII EUROPEJSKIEJ W ŚWIETLE UMOWY „TARCZA PRYWATNOŚCI" ORAZ PRAWODAWSTWA FEDERALNEGO USA

1. WPROWADZENIE

Usługi świadczone w formie elektronicznej podlegają coraz większej globalizacji, w rezultacie czego znaczna ich część obecnie ma charakter ponadnarodowy — przez co należy rozumieć nie tylko adresowanie ich do odbiorców zlokalizowanych w różnych krajach, lecz także korzystanie przy ich świadczeniu z podwykonawców i zasobów znacznie rozproszonych geograficznie.

Na tle rosnącego rynku e-usług coraz większego znaczenia nabiera zagadnienie zapewnienia zgodnego z prawem przetwarzania informacji udostępnionych przez użytkowników końcowych, w szczególności stanowiących dane osobowe. Problem ten jest szczególnie istotny w przypadku, gdy dane takie muszą być przekazywane transgranicznie, w konsekwencji czego pojawia się kwestia nie tylko różnych jurysdykcji, lecz często także różnych kultur prawnych[1].

* *Autor jest doktorantem Instytutu Nauk Prawno-Administracyjnych Uniwersytetu Warszawskiego.*

[1] „Transgraniczny przepływ danych" jest terminem stosowanym na określenie przekazywania zbiorów danych pomiędzy stronami znajdującymi się w różnych państwach i podlegających różnej jurysdykcji. Pojęcie to nie powinno być zawężane wyłącznie do wymiany danych w wersji elektronicznej, jednak z uwagi na znaczenie tej formy komunikacji (zarówno w wymiarze częstotliwości przekazywania, jak i wielkości zbiorów) stanowi ono bez wątpienia największy obszar zainteresowania prawodawców. Dlatego w niniejszym artykule przeanalizowano problematykę transgranicznej wymiany danych z perspektywy rynku cyfrowego i wymiany danych elektronicznych.

Wraz z reformą Unii Europejskiej, związaną z przyjęciem traktatu lizbońskiego[2], ochrona danych osobowych podniesiona została do rangi prawa podstawowego. Stało się tak na skutek uznania Karty praw podstawowych UE[3] (dalej: KPP) na mocy art. 6 ust. 1 Traktatu o Unii Europejskiej[4], jako części prawa pierwotnego UE. Gwarancje związane z ochroną danych osobowych zostały także wzmocnione poprzez wprowadzenie unijnej dyrektywy 95/46[5] z 1995 r., której głównym celem było ułatwienie integracji gospodarczej i funkcjonowania rynku wewnętrznego UE poprzez standaryzację poziomu ochrony pomiędzy państwami członkowskimi oraz wprowadzenie mechanizmów kontrolowania transgranicznego przepływu danych.

Model ochrony danych wprowadzony w UE przewiduje centralizację zarówno w obszarze przepisów prawa (unijna dyrektywa 95/46 wspólna dla wszystkich państw członkowskich, implementowana w postaci krajowych przepisów rangi ustawowej), jak i organów odpowiedzialnych za nadzór i kontrolę (krajowe, niezależne organy ochrony danych osobowych). Odmienny model przyjęto w Stanach Zjednoczonych. Różnice pojawiają się już na poziomie przepisów rangi konstytucyjnej — w USA prawo do prywatności, w tym ochrony danych osobowych, nie wynika wprost z konstytucji, zamiast tego zostało wprowadzone do systemu prawnego przez Sąd Najwyższy na drodze precedensowych orzeczeń dotyczących zakresu stosowania Czwartej Poprawki do Konstytucji[6]. W rezultacie, chociaż jako podstawę ochrony prywatności wskazuje się Czwartą Poprawkę, faktyczny zakres zarówno przedmiotowy, jak i podmiotowy tego prawa wynika z wielu wyroków Sądu Najwyższego wydawanych od drugiej połowy XX w.[7]

Przepisy rangi ustawowej funkcjonujące w USA nie traktują zagadnienia ochrony prywatności kompleksowo; zamiast tego wprowadzono oddzielne gwarancje związane z poszczególnymi obszarami (np. ochrona danych medycznych, telekomunikacyjnych itp.) lub rodzajem przetwarzania (np. ochrona danych przesyłanych w formie elektronicznej). Niejednolity system prawny funkcjonujący w USA — składający się z prawa federalnego oraz stanowego — dodatkowo utrudnia wywodzenie gwarancji ochrony praw związanych z danymi osobowymi. Uwzględnienia wymagają także prerogatywy władzy wykonawczej (prezydenta) związane w szczególności z obszarem bezpieczeństwa narodowego, na podstawie których może wydawać instrukcje i zarządzenia dla administracji rządowej wpływające wprost na efektyw-

[2] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 grudnia 2007 r. (Dz. Urz. UE C 306 z 2007 r., s. 1).

[3] Karta praw podstawowych Unii Europejskiej z dnia 30 marca 2010 r. (Dz. Urz. UE C 83 z 2010 r., s. 389).

[4] Dz. Urz. UE C 202 z 2016 r.

[5] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. UE L 281 z 1995 r., s. 31); w zakresie celów wprowadzenia por. treść motywu 5.

[6] Wyrok Sądu Najwyższego USA z dnia 7 czerwca 1965 r. w sprawie *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[7] K. Motyka: *Prawo do prywatności*, Zeszyty Naukowe Akademii Podlaskiej w Siedlcach, Seria Administracja i Zarządzanie, 2010, nr 85, s. 14.

ną skuteczność istniejących mechanizmów ochrony prywatności. Także obszar nadzoru i kontroli nie jest w USA sprawowany centralnie, w konsekwencji czego różne agendy rządowe wykonują działania związane z nadzorem przestrzegania przepisów dotyczących ochrony danych osobowych w nadzorowanych podmiotach[8].

W rezultacie wypracowanie przez UE i USA wspólnych zasad prawnych, gwarantujących podobny poziom ochrony danych osobowych, jest złożonym problemem prawnym. Transgraniczny przepływ danych jest jednak koniecznym warunkiem rozwoju handlu międzynarodowego, dlatego podjęte zostały działania, których skutkiem było przyjęcie programów „Bezpieczna przystań", a później „Tarcza prywatności" — pozwalających na przekazywanie danych osobowych przez administratorów danych mających siedzibę w UE do podwykonawców (odbiorców) przetwarzających dane na ich zlecenie na terenie Stanów Zjednoczonych.

2. ZASADY PRZEKAZYWANIA DANYCH OSOBOWYCH Z UNII EUROPEJSKIEJ DO PAŃSTW TRZECICH

Krajowy prawodawca uregulował kwestię transgranicznego przekazywania danych osobowych w art. 47 i n. ustawy o ochronie danych osobowych[9] (dalej: u.o.d.o.). Przepisy stanowią implementację dyrektywy 95/46, dlatego w ich redakcji odniesiono się do przekazywania danych do państw trzecich. Unijny prawodawca przez pojęcia państw trzecich rozumie kraje nienależące do UE oraz niebędące stronami układu o EOG[10]. Problem transgranicznego przekazywania danych szczegółowo uregulowano także w rozporządzeniu 2016/679[11] (dalej także jako ogólne rozporządzenie), które zacznie być stosowane od 25 maja 2018 r.[12]

Aby ułatwić realizację wymiany informacji i świadczenie usług, których elementem jest przekazywanie danych osobowych poza obszar UE[13], w dyrektywie 95/46 przewidziano możliwość wydawania przez Komisję Europejską decyzji o uznaniu, że dane państwo trzecie zapewnia odpowiedni stopień ochrony, adekwat-

[8] G. Shaffer: *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards*, Yale Journal of International Law 2000, t. 25, s. 31–32.

[9] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 ze zm.).

[10] Por. uzasadnienie do proponowanego art. 26 w: „Poprawiona propozycja Dyrektywy Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych", Komisja Europejska, COM (92) 422 final, s. 34.

[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (Dz. Urz. UE L 119 z 2016 r., s. 1).

[12] Por. art. 99 ust. 2 rozporządzenia 2016/679.

[13] Zarówno dyrektywa 95/46, jak i rozporządzenie 2016/679 mają zastosowanie do EOG, dlatego przedstawione rozważania pozostają aktualne nie tylko w odniesieniu do transferów do państw trzecich z terenu UE, lecz także w odniesieniu do transferów realizowanych przez administratorów z państw-stron EOG, nienależących do UE (Islandia, Liechtenstein, Norwegia).

ny do prawa unijnego w zakresie ochrony życia prywatnego, podstawowych praw i wolności osób fizycznych (tzw. decyzja o adekwatności). Wydanie takiej decyzji oznacza, że spełniona jest przesłanka pozytywna transferu danych, o której mowa w art. 47 ust. 1 u.o.d.o., czego praktyczną konsekwencją jest brak obowiązku występowania o indywidualną decyzję do organu nadzoru (GIODO)[14]. Wydanie decyzji indywidualnej w sytuacji objęcia państwa trzeciego istniejącą decyzją KE czyni postępowanie przed GIODO bezprzedmiotowym[15]. Stąd wniosek, że ocena Komisji Europejskiej w zakresie systemu prawnego państwa trzeciego i gwarancji, jakie są związane z ochroną prywatności i praw jednostek, ma doniosłe znaczenie praktyczne dla obrotu gospodarczego.

Lista decyzji wydanych przez KE jest dostępna publicznie na stronie internetowej[16]. Według stanu na 1 grudnia 2017 r. wydano 12 tego typu decyzji, w tym dotyczącą USA — będącą konsekwencją uzgodnienia pomiędzy KE a rządem USA warunków programu „Tarcza prywatności".

Należy podkreślić, że decyzja KE wydana w odniesieniu do Stanów Zjednoczonych określa warunki, jakie musi spełnić podmiot, który zamierza przetwarzać dane osobowe pochodzące z UE — w szczególności warunkiem tym jest przystąpienie do programu „Tarcza prywatności". Z przepisu art. 25 ust. 6 dyrektywy 95/46 wynika, że podstawę do wydania decyzji o adekwatności zabezpieczeń powinny być zabezpieczenia wynikające z „prawa krajowego lub międzynarodowych zobowiązań" państwa trzeciego. Istnieją poważne wątpliwości, czy warunek ten może być uznany za spełniony w przypadku, gdy program „Tarcza prywatności" jest opcjonalny (przystąpienie do niego jest dobrowolne), a regulacje w nim obowiązujące nie wynikają z przepisów prawa powszechnie obowiązującego.

Również rozpoczęcie stosowania przepisów ogólnego rozporządzenia nie będzie automatycznie skutkowało utratą ważności lub zmianą sposobu interpretacji wydanych wcześniej decyzji o adekwatności zabezpieczeń, w tym decyzji stanowiącej podstawę realizacji programu „Tarcza prywatności". Wynika to z faktu

[14] Wydanie decyzji o adekwatności zabezpieczeń nie jest jedyną podstawą formalną do przekazywania danych poza obszar UE/EOG bez konieczności uzyskiwania indywidualnej zgody krajowego organu nadzoru. Transfery takie mogą być realizowane także poprzez uwzględnienie tzw. standardowych klauzul umownych (art. 26 ust. 4 dyrektywy 95/46 oraz art. 46 ust. 2 pkt c–d rozporządzenia 2016/679) czy zatwierdzenia wiążących reguł korporacyjnych (art. 46 ust. 2 pkt b rozporządzenia 2016/679). Możliwość stosowania wiążących reguł korporacyjnych nie wynika wprost z przepisów dyrektywy — mechanizm ten został wprowadzony w drodze opinii i rekomendacji Grupy Roboczej Art. 29. Należy jednak podkreślić, że z wymienionych środków wydanie decyzji o adekwatności zabezpieczeń wiąże się z najpoważniejszymi konsekwencjami, znosi bowiem obowiązek podejmowania dodatkowych działań przez administratorów danych podejmujących transfery do państwa trzeciego. Omówienie obowiązujących na gruncie dyrektywy 95/46 podstaw przekazywania danych osobowych do państwa trzeciego w: M. Rojszczak: *Ochrona tajemnicy adwokackiej a usługi świadczone w chmurze obliczeniowej*, Studia Prawnicze 2017, nr 2, s. 164–168.

[15] Por. np. uzasadnienie decyzji GIODO z dnia 27 października 2015 r. (DESIWM/DEC-854/15) oraz z 10 września 2014 r. (DESIWM/DEC-886/14).

[16] *Commission decisions on the adequacy of the protection of personal data in third countries*, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (wszystkie odnośniki do publikatorów internetowych aktualne na dzień 1 grudnia 2017 r.).

wprowadzenia przez prawodawcę unijnego przepisu przejściowego art. 45 ust. 9 rozporządzenia 2016/679, zgodnie z którym decyzje podjęte przez Komisję na mocy art. 25 ust. 6 dyrektywy 95/46 pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia. W rezultacie przedstawione w niniejszym artykule rozważania nie stracą na aktualności także po 25 maja 2018 r., a więc po rozpoczęciu stosowania przepisów ogólnego rozporządzenia.

3. „BEZPIECZNA PRZYSTAŃ" I PRZYCZYNY JEJ UNIEWAŻNIENIA

Historycznie pierwszym rozwiązaniem prawnym umożliwiającym transfer danych osobowych z obszaru UE do Stanów Zjednoczonych bez konieczności wydawania indywidualnych decyzji administracyjnych były zasady ochrony prywatności określone w ramach programu „Bezpieczna przystań" oraz wydana w oparciu o nie decyzja KE 2000/520 z dnia 26 lipca 2000 r.[17] Jakkolwiek decyzja ta została uznana za nieważną wyrokiem Trybunału Sprawiedliwości UE na skutek rozpatrzenia sprawy *Schrems*, to przeanalizowanie zasad związanych z „Bezpieczną przystanią" wydaje się konieczne w celu odpowiedniego zrozumienia faktycznej skuteczności gwarancji dla podmiotów danych przewidzianych w zastępującym go programie, tj. „Tarczy prywatności".

Podstawowym pojęciem koniecznym do wyjaśnienia, aby zrozumieć ideę „Bezpiecznej przystani", jest „samocertyfikacja". Zgodnie z założeniami programu przystąpienie do niego było dobrowolne i wiązało się z przyjęciem przez przedsiębiorcę amerykańskiego publicznie dostępnej polityki ochrony prywatności, w której zadeklarował, że przestrzega zasad bezpiecznego transferu danych osobowych i faktycznie stosuje się do tych zasad, a także poświadczeniem zgodności, realizowanej poprzez przedstawienie Departamentowi Handlu Stanów Zjednoczonych deklaracji (oświadczenia) potwierdzającego przestrzeganie zasad bezpiecznego transferu danych[18]. Zasady ochrony prywatności określone przez Departament Handlu, stanowiące załącznik nr 1 do decyzji 2000/520, określały warunki realizacji „Bezpiecznej przystani" i definiowały podstawowe zasady związane z przetwarzaniem danych osobowych — takie jak zasada określonego celu, obowiązki informacyjne względem podmiotu danych, prawa podmiotu danych — w tym prawo sprze-

[17] Decyzja Komisji 2000/520 z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani" oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz. Urz. UE L 215 z 2000 r., s. 7).

[18] Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE z dnia 23 listopada 2013 r., COM (2013) 847 final, CELEX: 52013DC0847, „Struktura bezpiecznego transferu danych", s. 3.

ciwu, dostępu oraz żądania sprostowania, jak również dotyczące obowiązków administratora danych, w tym związanych z podejmowaniem rozsądnych środków ostrożności w celu ochrony przed utratą, niewłaściwym lub nieuprawnionym wykorzystaniem, dostępem, ujawnieniem, zmianą lub zniszczeniem informacji osobowych. Zasady te były więc próbą przeniesienia podstawowych regulacji wynikających z dyrektywy 95/46 i wspólnych dla państw UE na podmioty przetwarzające dane, prowadzące działalność w Stanach Zjednoczonych.

Mechanizm samooceny, w oparciu o który zbudowano program „Bezpiecznej przystani", zakładał wyłącznie deklaratywne podejście do spełnienia wymagań określanych przez zasady programu. W szczególności wskazywano, że przywileje związane z udziałem w programie przysługują od dnia, w którym organizacja przedstawia swój certyfikat w Departamencie Handlu, potwierdzający, że będzie przestrzegać zasad programu[19]. Natomiast same zasady nie miały mocy prawa powszechnie obowiązującego, a ponieważ program był opcjonalny, wiązał jedynie podmioty do niego przystępujące i tylko w zakresie określonym w zasadach. Poświadczenia miały być składane corocznie i na ich podstawie Departament Handlu zobowiązał się prowadzić publicznie dostępny rejestr firm spełniających kryteria programu.

Poza zasadami programu oraz dokumentem przedstawiającym najczęstsze pytania i odpowiedzi, załącznikami do decyzji 2000/520 były opisy mechanizmów egzekwowania prawa w ramach „Bezpiecznej przystani" przysługujące Federalnej Komisji Handlu (FKH) oraz ogólny opis prezentujący podstawy prawne dochodzenia odszkodowań z tytułu naruszenia prywatności w prawie federalnym i stanowym[20]. Warto podkreślić, że w założeniach twórców programu nadzór nad wykonywaniem „Bezpiecznej przystani" miał być realizowany na podstawie istniejących przepisów nadzorczych związanych z ochroną konkurencji i konsumentów (ochrona przed nieuczciwymi i wprowadzającymi w błąd praktykami handlowymi), funkcjonujących w prawie federalnym USA[21].

W rezultacie „Bezpieczna przystań" była *de facto* amerykańskim programem samooceny przedsiębiorców, który Komisja Europejska uznała za wystarczający do wydania decyzji w sprawie zasad bezpiecznego transferu danych osobowych. Program nie był elementem prawa międzynarodowego (umowy pomiędzy UE a USA), co w konsekwencji oznacza, że nie korzystał z pierwszeństwa przed prawem krajowym (federalnym) na podstawie art. VI Konstytucji USA[22]. Nie przewidziano także

[19] Decyzja KE 2000/520, *op. cit.*, załącznik II, NZP 6 — samocertyfikacja, s. 15.

[20] Decyzja KE 2000/520, *op. cit.*, załącznik III: Przegląd egzekwowania bezpiecznej przystani, s. 26.

[21] D. Solove: *The Scope and Potential of FTC Data Protection*, The George Washington Law Review 2015, t. 83, s. 2235–2237.

[22] W Stanach Zjednoczonych funkcjonuje kilka prawnych mechanizmów zawierania umów międzynarodowych; wiążące akty prawnomiędzynarodowe można podzielić na dwie główne kategorie: traktaty oraz umowy zawierane przez władzę wykonawczą. Wśród umów zawieranych przez władzę wykonawczą można wyróżnić kilka kolejnych typów, zależnych od stopnia wcześniejszej wiedzy lub zgody wyrażonej przez poszczególne izby Kongresu USA. Co do zasady tylko ratyfikowane traktaty posiadają moc równą prawu federalnemu; umowy zawierane przez władzę wykonawczą mogą wiązać się z takim skutkiem w wewnętrznym systemie prawnym — w szczególności

żadnych uprawnień kontrolnych dla organów UE w zakresie faktycznego przestrzegania zasad przez amerykańskie firmy przystępujące do programu. Co więcej, zgodnie z informacją zawartą w załączniku IV pkt B decyzji 2000/520 dopuszczono wyjątek od obowiązku stosowania zasad „Bezpiecznej przystani" w przypadku kolizji z przepisami prawa stanowionego albo precedensami: „w przypadkach, gdy prawo amerykańskie nakłada sprzeczny obowiązek na organizacje amerykańskie, czy to działające w ramach „Bezpiecznej przystani" czy poza nią, muszą one przestrzegać tego prawa". W rezultacie dopuszczano sytuację, w której zasady ustalone w ramach „Bezpiecznej przystani" — i stanowiące podstawę do przekazywania danych do Stanów Zjednoczonych — nie byłyby stosowane w przypadku kolizji z prawem krajowym USA (federalnym lub stanowym). Ponadto w załączniku I decyzji wskazano, że stosowanie zasad może być ograniczone w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego oraz interesu publicznego. Tak szeroko zakreślone wyjątki stały w sprzeczności ze skutecznym zagwarantowaniem ochrony danych obywateli UE na poziomie nie niższym niż w Unii, co jest warunkiem wydania przez KE decyzji o adekwatności zabezpieczeń.

W założeniu, decyzja KE wydawana na podstawie art. 25 ust. 6 dyrektywy 95/46 powinna wiązać się z analizą systemu prawnego państwa trzeciego połączoną z wykazaniem, że przyjęte rozwiązania prawne są wystarczające do ochrony praw i wolności jednostek w stopniu nie gorszym niż obowiązujący w UE. W przypadku dotyczącej Stanów Zjednoczonych decyzji 2000/520, podstawą jej wydania nie było jednak prawo powszechnie obowiązujące — ale dobrowolny program samocertyfikacji utworzony przez jeden z działów administracji rządu Stanów Zjednoczonych. „Bezpieczna przystań" nie została poddana ścieżce legislacyjnej przewidzianej dla prawa federalnego, nie wprowadzała nowych obowiązków *ius cogens* w prawie amerykańskim. Powstawała zatem uzasadniona wątpliwość, czy KE, bazując na mechanizmach, które można określić jako *soft-law*, nie przekroczyła swoich uprawnień i była władna wydać decyzję skutkującą ułatwieniem w transferze danych do USA. W szczególności, art. 25 ust. 6 stanowiący podstawę kompetencyjną do wydania przez KE decyzji wymaga przeprowadzenia pozytywnej oceny „prawa krajowego lub międzynarodowych zobowiązań" — program „Bezpiecznej przystani" nie należy do żadnej z tych dwóch kategorii.

Oddzielnym problemem była możliwość skutecznej ochrony praw wynikających z programu przed sądami amerykańskimi przez obywateli UE. W tym zakresie,

w przypadku umów zawieranych za zgodą Kongresu lub dla wypełnienia innych zobowiązań traktatowych. Porozumienie „Bezpieczna przystań" bez wątpienia nie było traktatem, nie służyło wypełnieniu zobowiązań prawnomiędzynarodowych USA wynikających z innego traktatu, jak również w jego określeniu i zawarciu nie uczestniczył Kongres. Nie jest zatem umową międzynarodową nie tylko w rozumieniu prawa międzynarodowego, lecz także w wewnętrznym systemie prawnym USA. Więcej informacji na temat rodzajów umów międzynarodowych funkcjonujących w amerykańskim systemie prawnym oraz zasad pierwszeństwa w przypadku kolizji z prawem wewnętrznym: M. Garcia: *International Law and Agreements — Their Effect upon U.S. Law*, Congressional Research Service 2015, http://cli.re/LvbD1M.

zgodnie z warunkami programu, podstawę stanowiły mechanizmy pozasądowego rozstrzygania sporów (ang. *alternative dispute resolution*, ADR). Każdy przedsiębiorca przystępujący do programu był zobowiązany do wskazania na swojej stronie internetowej podmiotu świadczącego usługi w zakresie ADR. Według danych Komisji opublikowanych w 2013 r. usługi te nie zawsze były bezpłatne, a ponieważ to przedsiębiorca wskazywał podmiot świadczący usługi ADR — takie rozwiązywanie sporów było nie zawsze dostępne finansowo dla obywateli UE[23]. W przypadku niepowodzenia arbitrażu ADR sprawa miała być przekazywana FKH, która następnie powinna wykorzystać swoje narzędzia nadzorcze w celu doprowadzenia do rozstrzygnięcia sporu. Dopiero w przypadku niepowodzenia ścieżki administracyjnej sprawa byłaby kierowana przez FKH na drogę postępowania sądowego. „Bezpieczna przystań" nie przewidywała więc prostej ścieżki dochodzenia swoich praw przed sądami powszechnymi. Na nieskuteczność procedury rozstrzygania sporów mogą wskazywać dane Komisji, według których w latach 2000–2013 żadna skarga na nieprzestrzeganie zasad programu nie została przekazana do rozpoznania przez FKH[24].

Wskazane wyżej wątpliwości stały się przedmiotem analizy TSUE w sprawie *Schrems*[25]. Tłem badanej sprawy były ujawnione w 2013 r. przez E. Snowdena programy masowej inwigilacji prowadzone przez amerykańskie agencje wywiadowcze, których jednym z podstawowych elementów było hurtowe przechwytywanie danych elektronicznych, w tym dotyczących obywateli UE[26]. W pierwszej kolejności Trybunał zauważył, że ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne[27]. W tym zakresie ustanowienie pierwszeństwa dla wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania amerykańskiego prawa przed zasadami „Bezpiecznej przystani" prowadziło do ingerencji w prawa podstawowe osób, których dane osobowe zostały lub mogły zostać przekazane z Unii do Stanów Zjednoczonych. Uregulowanie pozwalające władzom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych Trybunał uznał za prowadzące do naruszenia zasadniczej istoty prawa do poszanowania życia prywatnego, wynikającego z art. 7 KPP — co w rezultacie stało się podstawą stwierdzenia nieważności decyzji KE 2000/520[28].

[23] Komunikat Komisji do Parlamentu Europejskiego i Rady…, *op. cit.*, „Pozasądowe rozstrzyganie sporów", s. 17.

[24] *Ibidem*, s. 18.

[25] Wyrok TSUE z dnia 6 października 2015 r. w sprawie *Schrems*, C-362/14.

[26] Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, P7_TA(2014)0230.

[27] Wyrok TSUE z dnia 8 kwietnia 2014 r. w sprawie *Digital Rights Ireland Ltd*, C-293/12 i C-594/12, pkt 52.

[28] Wyrok TSUE w sprawie *Schrems*, pkt 86–87.

Trybunał wskazał ponadto na nieskuteczność przewidzianego w programie mechanizmu niezależnej ochrony prawnej. W szczególności kompetencje prywatnego arbitrażu oraz Federalnej Komisji Handlu ograniczone są do sporów handlowych i nie obejmują rozwiązywania sporów dotyczących legalności ingerencji realizowanej przez organy państwowe. Ta obserwacja miała zasadnicze znaczenie, biorąc pod uwagę, że naruszenia ujawnione przez E. Snowdena związane były z działalnością agend rządu USA (w szczególności Narodowej Agencji Bezpieczeństwa, NSA), a nie podmiotów prywatnych. W konsekwencji dochodzenie przez obywateli UE swoich praw w oparciu o wynikające z „Bezpiecznej przystani" mechanizmy prawne nie mogło być skuteczne i doprowadzić do usunięcia skutków naruszenia.

Ostatnią z przesłanek nieważności decyzji był brak wykazania przez Komisję, że przedsiębiorstwa uczestniczące w programie faktycznie zapewniają — a nie tylko deklarują poprzez mechanizm samooceny — odpowiedni stopień ochrony ze względu na swoje ustawodawstwo lub zobowiązania międzynarodowe[29].

Niezależnie od analizy programu „Bezpiecznej przystani" oraz wykazania przyczyn nieważności decyzji dotyczącej programu Trybunał zajął się także problemem uprawnień krajowych organów ochrony danych osobowych w zakresie możliwości kwestionowania wydanej przez KE decyzji o adekwatności zabezpieczeń. W tym zakresie TSUE stwierdził, że wydanie przez Komisję decyzji nie stoi na przeszkodzie temu, aby krajowy organ nadzorczy rozpatrzył skargę danej osoby dotyczącą ochrony jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, które zostały przekazane z państwa członkowskiego do państwa trzeciego, kiedy osoba ta podnosi, że obowiązujące w tym państwie trzecim prawo i praktyki nie zapewniają odpowiedniego stopnia ochrony[30].

W wyroku w sprawie *Schrems* nie tylko więc określono przesłanki, jakimi należy się kierować przy konstrukcji programów transferu danych osobowych, aby zachować zgodność z prawem UE, lecz także potwierdzono możliwość dochodzenia praw przez obywateli UE przed krajowymi organami ochrony danych osobowych oraz kwestionowania za ich pośrednictwem decyzji KE na drodze sądowej.

4. NOWY SCHEMAT OCHRONY PRAW JEDNOSTKI W UMOWIE „TARCZA PRYWATNOŚCI"

Stwierdzenie nieważności decyzji KE 2000/520 skutkowało brakiem podstawy prawnej do dalszego prowadzenia programu „Bezpieczna przystań". W jego miejsce wprowadzony został program „Tarcza prywatności", który na podstawie decyzji

[29] *Ibidem*, pkt 83.
[30] *Ibidem*, pkt 102–103.

wykonawczej KE 2016/1250 z dnia 12 lipca 2016 r.[31] stał się podstawą realizacji transgranicznego transferu danych osobowych do Stanów Zjednoczonych. Według danych na dzień 1 czerwca 2017 r., do programu przystąpiło 2245 amerykańskich przedsiębiorców[32].

Ogólne ramy programu pozostały niezmienione w porównaniu z „Bezpieczną przystanią" — w szczególności „Tarcza prywatności" jest także schematem bazującym na samoocenie podmiotów, które dobrowolnie mogą do niego przystąpić. Jednak z uwagi na tezy zawarte w wyroku TSUE w sprawie *Schrems* konieczne było uwzględnienie w nowej decyzji skutecznych rozwiązań następujących problemów:

a) pierwszeństwa prawa amerykańskiego nad zasadami programu oraz postępowania uczestników programu w przypadku sprzecznych norm prawa lub wymagań bezpieczeństwa narodowego z warunkami „Tarczy prywatności";
b) oceny, czy podmioty uczestniczące w programie faktycznie stosują zasady, które deklarują;
c) możliwości skutecznego dochodzenia praw przez obywateli UE.

Na wstępie omówienia pierwszego ze wskazanych zagadnień należy zauważyć, że „Tarcza prywatności" nadal nie stanowi elementu prawa międzynarodowego. Podobnie jak w przypadku „Bezpiecznej przystani", decyzja KE opiera się na założeniach opracowanych i przyjętych przez Departament Handlu USA, uzupełnionych zestawem oświadczeń i deklaracji przedstawicieli rządu USA. Oświadczenia te bez wątpienia nie mają jednak mocy traktatu międzynarodowego, ustalenia w nich zawarte podobnie jak w przypadku „Bezpiecznej przystani" nie podlegały procedurze ratyfikacji przewidzianej przez konstytucję oraz przepisy federalne. Chociaż w systemie prawnym Stanów Zjednoczonych istnieje kilka alternatywnych procedur prowadzących do ratyfikacji umowy międzynarodowej, każda z nich zakłada wyrażenie zgody przez prezydenta, a w niektórych przypadkach także przez większość obu izb kongresu lub 2/3 senatorów[33]. Bez wątpienia dokumenty przedstawione przez rząd USA i załączone do decyzji 2000/520 nie zostały poddane takiej procedurze legislacyjnej, w związku z czym nie korzystają z tzw. klauzuli pierwszeństwa, zgodnie z którą w systemie prawnym USA ratyfikowane umowy międzynarodowe są zrównane rangą z prawem federalnym[34].

Ponadto należy wskazać, że deklaracje przedstawicieli władzy wykonawczej USA prezentują stanowisko administracji na dzień ich złożenia. W szczególności dotyczy to zapewnień i gwarancji wynikających z wydanych dyrektyw prezydenta, które mogą być w każdej chwili cofnięte lub zmodyfikowane przez każdego kolejnego prezydenta USA. Dlatego w tym zakresie nie można zgodzić się ze stanowi-

[31] Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę prywatności UE-USA, CELEX: 32016D1250.

[32] *Privacy Shield List*, https://www.privacyshield.gov/list.

[33] M. Garcia: *International Law…*, *op. cit.*, s. 4–6.

[34] Por. informacje zawarte w przyp. 22.

skiem Komisji Europejskiej[35], która przyjmuje deklaracje ze strony Urzędu Dyrektora Krajowych Służb Wywiadowczych dotyczące zakazu prowadzenia masowych i nieukierunkowanych programów wywiadowczych nastawionych na pozyskanie i przetwarzanie hurtowych zbiorów danych osobowych jako wystarczające do zagwarantowania, że takie programy nie powstaną w przyszłości na mocy istniejących w amerykańskim systemie prawnym przepisów ustawowych.

Ramowe zasady „Tarczy prywatności", wydane przez Departament Handlu i stanowiące załącznik nr 2 do decyzji KE 2016/1250, podobnie jak w przypadku „Bezpiecznej przystani", przewidują możliwość odstąpienia od warunków programu w przypadku sprzeczności między innymi z wymogami bezpieczeństwa narodowego, interesu publicznego lub egzekwowania prawa[36]. Ponadto ustalono, że w zakresie wykładni oraz zagadnień związanych z przestrzeganiem zasad oraz odpowiednich polityk ochrony prywatności stosowane będzie prawo amerykańskie — chyba że podmiot przystępujący do programu zgodzi się na uznanie prawa państwa członkowskiego UE. Chociaż „Tarcza prywatności" zawiera wiele wyjaśnień i oświadczeń dotyczących ograniczeń obowiązujących organy władzy publicznej w hurtowym dostępie do danych osobowych, żadna z tych informacji nie ma charakteru prawotwórczego. Dlatego należy uznać, że istnieje duże prawdopodobieństwo, iż postanowienia „Tarczy prywatności" zostaną uznane za niewystarczające i prowadzące do naruszenia prawa UE w przypadkach, w których pozwalają na zastosowanie sprzecznych norm prawa federalnego.

Drugie z zagadnień, które wymaga omówienia w kontekście wcześniejszego wyroku TSUE w sprawie *Schrems*, to kwestia zapewnienia, że podmioty uczestniczące w programie faktycznie stosują zasady, a nie tylko deklarują ich przestrzeganie. W tym zakresie Departament Handlu zadeklarował, że będzie prowadził regularne aktualizacje listy i przeglądy dokumentacji przekazanej przez uczestniczące przedsiębiorstwa w celu zapewnienia, by przestrzegały one zasad, którym się podporządkowały. Zgodnie z informacją zawartą w Ramowych zasadach „Tarczy prywatności", podmioty uczestniczące w programie muszą zapewnić procedury kontrolne pozwalające sprawdzić, czy ich poświadczenia i zapewnienia dotyczące praktyk ochrony prywatności są prawdziwe oraz czy praktyki te zostały wdrożone tak, jak zostało to przedstawione oraz zgodnie z zasadami „Tarczy prywatności"[37]. Jak jednak doprecyzowano w dalszej części dokumentu, poświadczenia takie mogą mieć formę zewnętrznych przeglądów zgodności (audytów), ale również mogą być realizowane w drodze samooceny. Mechanizm zewnętrznych audytów nie jest zatem elementem obowiązkowym i jego zastosowanie zależy od decyzji podmiotu. Bez

[35] Komunikat prasowy Komisji Europejskiej z dnia 12 lipca 2016 r., „Komisja Europejska uruchamia Tarczę Prywatności UE-USA: lepsza ochrona transatlantyckiego przepływu danych", IP/16/2461, europa.eu/rapid/press-release_IP-16-2461_pl.htm.

[36] Decyzja KE 2016/1250, *op. cit.*, załącznik II, pkt I.5.

[37] Decyzja KE 2016/1250, *op. cit.*, załącznik II, pkt III.7.

okresowych przeglądów zewnętrznych — czy to realizowanych przez firmy audytorskie, czy organy nadzoru — prawdziwość deklaracji uczestników programu „Tarcza prywatności" nie będzie weryfikowana w niezależny sposób. Istnieje zatem ryzyko, że zaproponowany mechanizm okresowej samooceny nie sprosta wymaganiu TSUE wprowadzenia skutecznego mechanizmu wykrywania i kontroli, pozwalającego na identyfikowanie i ukaranie podmiotów naruszających warunki programu[38].

Ostatni z obszarów zakwestionowanych w warunkach programu „Bezpieczna przystań", który z pewnością stanie się przedmiotem sądowej kontroli w zakresie „Tarczy prywatności", dotyczy możliwości skutecznego dochodzenia swoich praw przez obywateli UE. Rozwiązanie skarg i sporów wprowadzone w „Tarczy prywatności" składa się z trzech alternatywnych ścieżek postępowania:

- złożenie skargi w podmiocie przetwarzającym dane, który ma 45 dni na jej rozpatrzenie;
- skorzystanie z bezpłatnej usługi pozasądowego rozwiązywania sporów, świadczonej przez firmę wskazaną (wybraną) przed podmiot uczestniczący w programie;
- skierowanie skargi do organu ochrony danych osobowych państwa członkowskiego UE, która następnie zostanie przesłana do Departamentu Handlu; skarga powinna być rozpatrzona w ciągu 90 dni lub, jeżeli jest to niemożliwe, skierowana do Federalnej Komisji Handlu.

Tylko trzeci z zaproponowanych mechanizmów jest zupełnie nowy w porównaniu z programem „Bezpieczna przystań" — dwa pierwsze istniały już wcześniej, zmodyfikowano tylko warunki ich realizacji (np. poprzez zobowiązanie, że pozasądowe rozstrzyganie sporów musi być realizowane bezpłatnie dla skarżącego). Należy jednak pamiętać, że podstawą rozstrzygania sporów (poza wyjątkami dotyczącymi spraw pracowniczych) będzie prawo amerykańskie, w tym także amerykańskie prawo procesowe. W tym zakresie „Tarcza prywatności" nie wprowadza prostego i dostępnego mechanizmu stosowania przepisów UE. Także zaangażowanie unijnych organów nadzoru ogranicza się do pośrednictwa w przekazywaniu skarg do Departamentu Handlu.

W przypadku, w którym podmiot przystępujący do programu zamierza także przetwarzać dane związane z zatrudnieniem (informacje pracownicze), obowiązkowo musi współpracować z organem ochrony danych osobowych państwa członkowskiego, nie wyłączając obszaru przyjmowania skarg i rozwiązywania sporów[39].

„Tarcza prywatności" wprowadza jeszcze jeden, nowy mechanizm rozstrzygania sporów — jest nim panel arbitrażowy ustanowiony na podstawie załącznika 1 do załącznika II decyzji 2016/1250. Zgodnie z warunkami programu, do rozstrzygnięcia przez panel arbitrażowy mogą być kierowane sprawy, które były przedmiotem jednego z trzech wymienionych wcześniej mechanizmów ochrony prawnej. W skład panelu

[38] Wyrok TSUE w sprawie *Schrems*, pkt 81.

[39] Decyzja KE 2016/1250, *op. cit.*, załącznik III, pkt 9.d.2.

arbitrażowego wchodzi co najmniej 20 arbitrów powoływanych wspólnie przez Departament Handlu i Komisję Europejską, przy czym indywidualne sprawy będzie rozpatrywał panel złożony z jednego lub trzech arbitrów. Panel do spraw „Tarczy prywatności" będzie uprawniony do przyznania „godziwego środka naprawiającego szkodę w formie niepieniężnej"[40], a orzeczenia arbitrażowe będą mogły być egzekwowane przed sądami federalnymi. W ramach arbitrażu nie przewidziano możliwości dochodzenia zadośćuczynienia czy zwrotu kosztów, w tym kosztów zastępstwa procesowego. Ponadto z jego zakresu wyłączone zostały sprawy dotyczące stosowania wyjątków od reguł „Tarczy prywatności", czyli na przykład spraw związanych z odstąpieniem od zasad programu z uwagi na kolizję z wymaganiami bezpieczeństwa narodowego[41].

Jak wskazała Grupa Robocza Art. 29 w swojej opinii dotyczącej projektu decyzji 2016/1250 oraz programu „Tarcza prywatności", jakość mechanizmów ochrony prawnej powinna mieć większą wagę niż ich liczba[42]. Należy zwrócić uwagę, że każdy z mechanizmów ma inną podstawę formalną funkcjonowania, wynikającą z odrębnych dokumentów (często stanowiących deklarację innego urzędu USA). Takie podejście do rozwiązywania sporów jest nieczytelne, trudne w ocenie i późniejszej analizie skuteczności.

Odrębną kwestią jest odpowiedzialność przekazującego dane, a więc podmiotu europejskiego, za niezgodne z warunkami programu przetwarzanie prowadzone przez partnera amerykańskiego. Należy przypomnieć, że regulacje dotyczące transgranicznego przekazywania danych nie wyłączają ani nie ograniczają ogólnych przepisów kształtujących odpowiedzialność administratora danych za zgodne z prawem przetwarzania, w tym także za odpowiednie powierzenie danych do przetwarzania. Decyzja o adekwatności zabezpieczeń zwalnia z potrzeby uzyskiwania indywidualnej decyzji organu nadzoru. Nie prowadzi jednak do braku konieczności spełnienia wymagań związanych z powierzeniem przetwarzania danych konkretnemu podmiotowi. Dlatego w doktrynie wyróżnia się umowy transferowe oraz umowy na powierzenie przetwarzania danych. W przypadku Privacy Shield podmioty europejskie nie mają potrzeby zawierania umów transferowych (zastępuje je decyzja o adekwatności zabezpieczeń — w analizowanym przypadku decyzja KE 2016/1250). W dalszym ciągu jednak przekazanie danych musi nastąpić w oparciu o umowę powierzenia przetwarzania danych[43]. Dlatego kwestia odpowiedzialności administratora danych za naruszenia dokonane przez partnera amerykańskiego (w szcze-

[40] *Ibidem*, załącznik 1 do załącznika I, pkt B.

[41] *Ibidem*, załącznik 1 do załącznika I, pkt A.

[42] Grupa Art. 29 ds. Ochrony Danych, *Opinion 01/2016 on the EU — U.S. Privacy Shield draft adequacy decision*, 13.04.2016, WP 238, ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.

[43] Obowiązek zawarcia umowy powierzenia przetwarzania danych wynika wprost z regulacji krajowych (art. 31 ust. 1 u.o.d.o.) oraz unijnych (por. art. 17 ust. 3 dyrektywy 95/46 oraz art. 28 ust. 3 ogólnego rozporządzenia). Z kolei podmioty amerykańskie uczestniczące w programie „Tarcza prywatności" zobowiązane są do zawarcia takiej umowy na mocy pkt II–10 załącznika I decyzji 2016/1250.

gólności przetwarzanie niezgodne z warunkami programu Privacy Shield) wymaga odniesienia do przepisów szczególnych — wynikających zarówno z prawa ochrony danych, ochrony konsumentów, jak i norm prawnomiędzynarodowych w zakresie odpowiedzialności za zobowiązania oraz delikty[44].

Nie powinno natomiast budzić wątpliwości, że ramowe zasady programu „Tarcza prywatności" — opisane w załącznikach do decyzji 2016/1250 (w szczególności w załączniku II) nie tworzą nowych obowiązków dla podmiotów europejskich (administratorów danych), a także nie mają bezpośredniego skutku horyzontalnego w relacjach pomiędzy jednostkami[45]. Niezależnie od charakteru prawnego tych załączników (zob. wcześniejsze rozważania), z literalnego brzmienia pkt I.1 załącznika II wynika, że „są one przeznaczone do wyłącznego użytku amerykańskich podmiotów otrzymujących dane osobowe z Unii Europejskiej". Zasady pozostają bez wpływu na zobowiązania podmiotów europejskich wynikających z właściwych przepisów krajowych oraz unijnych[46].

Zgodnie z pkt I.7 załącznika I właściwe do interpretacji i wykładni zagadnień związanych z przestrzeganiem zasad jest prawo amerykańskie. Próba poszukiwania w dokumentach załączonych do decyzji 2016/1250 źródeł obowiązków dla europejskich administratorów danych napotkałaby zatem także trudność związaną z koniecznością zastosowania obcego systemu prawnego, co samo w sobie prowadziłoby do naruszenia przepisów zarówno decyzji 2016/1250, jak i aktów prawa wyższego rzędu (w szczególności dyrektywy 95/46 oraz rozporządzenia 2016/679).

5. PRAWO DO PRYWATNOŚCI REZYDENTÓW UNII EUROPEJSKIEJ NA GRUNCIE PRAWA FEDERALNEGO

Analiza możliwości egzekwowania gwarancji wynikających z „Tarczy prywatności" i ich praktycznego znaczenia w amerykańskim systemie prawnym wymaga przedstawienia kluczowych przepisów prawa federalnego. Ponieważ wątpliwości podniesione przez TSUE związane z realizacją programu „Bezpieczna przystań" dotyczyły w dużej mierze braku kontroli nad władzą publiczną w dostępie do danych przekazywanych do USA, w pierwszej kolejności należy przeanalizować, na ile

[44] Szersze omówienie problematyki w: M. Kolasiński, M. Świerczyński: *Wybór prawa obcego w internetowych wzorcach umownych — obowiązek spojrzenia na ochronę konsumentów z perspektywy prawa prywatnego międzynarodowego* (w:) *Prawo konsumenckie w praktyce*, pod red. M. Czarneckiej, T. Skocznego, Warszawa 2016; M. Jagielska, A. Kunkiel-Kryńska: *Wybór prawa jako klauzula abuzywna w umowach konsumenckich zawieranych przez Internet*, IKAR 2016, nr 3, s. 4; A. Jaroszek: *Ważność wyboru* (w:) A. Jaroszek: *Prawo właściwe dla umów konsumenckich zawieranych przez Internet*, Warszawa 2009.

[45] Zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 202 z 2016 r.; dalej TFUE), decyzja, która wskazuje adresatów, wiąże tylko tych adresatów. Decyzja 2016/1250 jest adresowana do państw (art. 6). TSUE wypowiadał się na temat możliwego bezpośredniego skutku wertykalnego decyzji adresowanych do państw (por. wyrok TSUE z dnia 10 listopada 1992 r. w sprawie *Hans Fleisch*, C-156/91).

[46] Por. art. 2 decyzji 2016/1250.

istniejące prawo pozwala na faktyczne ominięcie gwarancji związanych z ochroną prywatności przewidzianych w „Tarczy prywatności".

Konstytucja USA nie wprowadza wprost gwarancji związanych z ochroną prywatności. Podstawę do formułowania tego prawa stanowi Czwarta Poprawka, dotycząca nietykalności osobistej i materialnej oraz zakazująca przeprowadzania nieuzasadnionych rewizji lub zatrzymań[47]. W drodze precedensowych orzeczeń Sądu Najwyższego USA na podstawie Czwartej Poprawki wywiedziono gwarancje związane z ochroną prywatności, obejmujące także informacje zapisane na nośnikach elektronicznych[48]. Należy jednak zauważyć, że zakres przedmiotowy stosowania Czwartej Poprawki w przypadku ochrony danych powierzonych do przetwarzania w systemach usługodawców (np. systemy bankowe, telekomunikacyjne, dane przetwarzane w chmurze obliczeniowej) jest znacznie ograniczony, co wynika z obowiązującej w amerykańskiej doktrynie testu „uzasadnionego oczekiwania prywatności". Zgodnie z podejściem pierwotnie wprowadzonym w sprawie *Katz v. Stany Zjednoczone*[49] ustalenie, czy działania władzy publicznej naruszają Czwartą Poprawkę, odbywa się dwuetapowo. W pierwszym sąd powinien ocenić, czy ingerencja narusza subiektywne oczekiwanie prywatności, a więc przekonanie jednostki, że nastąpiło wkroczenie w jej sferę prywatności. Dopiero jeżeli odpowiedź na pierwsze pytanie jest twierdząca, sąd powinien rozważyć, czy oczekiwanie jest obiektywnie uzasadnione, a więc czy „społeczeństwo jest gotowe, aby uznać je za uzasadnione"[50]. Ponieważ obszar subiektywnych odczuć jednostki nie podlega prostej ocenie, w amerykańskiej judykaturze przyjmuje się, że zasadniczym elementem testu jest wyważenie tego, co obiektywnie można uznać za „uzasadnione"[51]. W orzecznictwie sądów federalnych wskazuje się między innymi na brak spełnienia przesłanki uzasadnionego oczekiwania prywatności w przypadkach, gdy jednostka dobrowolnie przyczyniła się do upowszechnienia informacji. Przykładem takiego upowszechnienia może być w ocenie A. Gold skorzystanie z usług przetwarzania w chmurze obliczeniowej[52]. W piśmiennictwie wyrażane są jednak także poglądy odmienne, wskazujące na rosnące znaczenie powszechnego (obiektywnego) oczekiwania prywatności w korzystaniu z usług świadczonych w chmurze[53].

[47] Tekst polski: http://libr.sejm.gov.pl/tek01/txt/konst/usa.html.

[48] A. Gold: *Obscured by clouds: the Fourth Amendment and searching cloud storage accounts through locally installed software*, William & Mary Law Review 2015, t. 6, s. 2327–2328.

[49] Wyrok Sądu Najwyższego USA z dnia 18 grudnia 1967 r., sprawa *Stany Zjednoczone v. Katz*, 389 U.S. 347 (1967).

[50] *Ibidem*, s. 361; szersze omówienie testu uzasadnionego oczekiwania prywatności — A. Czubik: *Prawo do prywatności. Wpływ amerykańskich koncepcji i rozwiązań prawnych na prawo międzynarodowe*, Kraków 2013, s. 153–157.

[51] O. Kerr: *The Fourth Amendment in cyberspace: can encryption create a resonable expectation of privacy?*, Connecticut Law Review 2001, t. 33, s. 507.

[52] A. Gold: *Obscured…*, *op. cit.*, s. 2339–2340.

[53] E. Johnson: *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, Stanford Law Review 2017, t. 69, s. 885–887.

W zakresie podmiotowym gwarancje przewidziane w Czwartej Poprawce nie mają zastosowania do czynności przeszukania realizowanych w odniesieniu do osoby niebędącej amerykańskim rezydentem. Wniosek taki wynika z orzeczenia SN w sprawie *Stany Zjednoczone v. Verdugo-Urquidez*[54] i jest często przytaczany w literaturze przedmiotu w kontekście wskazania ograniczonych gwarancji dla obywateli UE w zakresie prawa do poszanowania prywatności[55]. W rezultacie praktyczne znaczenie Czwartej Poprawki w odniesieniu do ochrony danych obywateli UE przetwarzanych w systemach informatycznych amerykańskich usługodawców jest niewielkie[56].

Ustawą wprowadzającą prawa i gwarancje związane z przetwarzaniem danych przez administrację publiczną, najbardziej odpowiadającą europejskim przepisom o ochronie danych, jest Privacy Act z 1974 r.[57] Celem aktu jest wprowadzenie podstawowych gwarancji związanych z gromadzeniem, przetwarzaniem i ujawnianiem wszelkich typów danych osobowych, w tym danych dotyczących stanu zdrowia i innych danych wrażliwych, przez agencje rządu federalnego, nie wyłączając organów ścigania. Ustawa określa wiele rozwiązań i mechanizmów znanych z europejskich przepisów o ochronie danych, w tym obowiązek publicznego ogłoszenia o prowadzeniu bazy danych (odpowiednik zgłoszenia do GIODO w polskich przepisach[58]), obowiązki informacyjne względem osób, których dane są przetwarzane, a także prawa jednostek do dostępu czy poprawiania danych.

Ponieważ Privacy Act jest ustawą federalną, nie ma zastosowania do działań władz stanowych w zakresie przetwarzania danych osobowych. Nie wszystkie stany uchwaliły swoje przepisy w tym obszarze. Standaryzacja przepisów stanowych jest zapewniona tylko w obszarach wymaganych przez prawo federalne. W pozostałym zakresie legislatorzy mogą i stosują odmienne modele ochrony danych, czego skutkiem są różne przepisy lokalne obowiązujące w poszczególnych stanach[59].

Naruszenia przepisów ustawy Privacy Act mogą być dochodzone na drodze sądowej. W szczególności osoby, których prawa naruszono, mogą dochodzić odszkodowania oraz zadośćuczynienia w postępowaniu cywilnym[60]. Dodatkowo urzędnicy odpowiedzialni za umyślne działania, skutkujące naruszeniem przepisów ustawy, mogą zostać ukarani na drodze dyscyplinarnej lub sądzeni w postępowaniu karnym[61].

[54] Wyrok Sądu Najwyższego USA z dnia 28 lutego 1990 r., sprawa *Stany Zjednoczone v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

[55] Directorate General for Internal Policies Policy, Department C: Citizens' Rights and Constitutional Affairs: „The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens", Bruksela 2015, dostęp: www.europarl.europa.eu/studies, rozdział 2.1, s. 10.

[56] Szersze rozważania dotyczące stosowania gwarancji konstytucyjnych USA wobec obcokrajowców — D. Cole: *Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens?*, Thomas Jefferson Law Review 2003, t. 25, s. 367–388.

[57] Ustawa federalna USA z dnia 31 grudnia 1974 r. o ochronie prywatności (Privacy Act); 93–579, publikacja 5 U.S.C. § 552a.

[58] Por. art. 40 u.o.d.o.

[59] G. Shaffer: *Globalization…*, *op. cit.*, s. 29–30.

[60] 5 U.S.C. § 552a(g).

[61] 5 U.S.C. § 552a(h).

Należy zwrócić uwagę, że zakres podmiotowy stosowania Privacy Act jest istotnie ograniczony. W szczególności ustawa obejmuje wyłącznie dane przetwarzane przez podmioty mające według prawa federalnego status agencji rządowej, nie obejmuje zatem innych organów władzy wykonawczej, sądowniczej czy prawodawczej. Ponadto zawiera szereg wyłączeń, dotyczących w szczególności uprawnień i obowiązków związanych z gromadzeniem i przetwarzaniem danych w celu zapewnienia bezpieczeństwa i stosowania prawa. Należy także podkreślić, że stosowanie przepisów ustawy obejmuje wyłącznie obywateli lub rezydentów posiadających prawo pobytu na terenie Stanów Zjednoczonych[62]. Ustawa Privacy Act nie nadaje zatem żadnych praw ani gwarancji obcokrajowcom (w tym i obywatelom UE) związanych z przetwarzaniem ich danych przez agencje rządu federalnego USA.

Brak możliwości dochodzenia przez osoby z UE praw przed sądami amerykańskimi, związanych z naruszeniem prywatności czy ochrony danych osobowych przez władze USA, było jedną z przyczyn uchwalenia w 2015 r. ustawy Judicial Redress Act (dalej: JRA)[63]. Przepisy ustawy weszły w życie 1 lutego 2017 r., a ich podstawowym celem jest rozszerzenie kręgu osób uprawnionych z Privacy Act na obywateli innych państw lub regionalnych organizacji ekonomicznych, których lista ma być okresowo aktualizowana przez Biuro Prokuratora Generalnego USA. Podstawą do umieszczenia na liście jest współpraca z USA:

1) w sprawach karnych w związku z zapobieganiem, wykrywaniem i ściganiem przestępstw oraz
2) zgoda wynikająca z zawartej umowy międzynarodowej lub innej podstawy prawnej na transfer danych osobowych w celach komercyjnych na terytorium Stanów Zjednoczonych.

W przypadku UE pierwsza przesłanka jest realizowana w wyniku zawartej umowy międzynarodowej[64] dotyczącej wymiany danych przez organy egzekwowania prawa w związku z prowadzonymi postępowaniami karnymi (zwana w literaturze przedmiotu także „umową parasolową UE–USA")[65], natomiast druga przesłanka jest spełniona poprzez zatwierdzenie warunków programu „Tarcza prywatności". W rezultacie, 23 stycznia 2017 r. w federalnym dzienniku urzędowym opublikowane zostało zarządzenie[66] wyznaczające państwa członkowskie (z wyłączeniem Danii i Wielkiej Brytanii[67]) oraz UE, będącą organizacją międzynarodową, jako objęte postanowieniami ustawy.

[62] 5 U.S.C. § 552a(a)(2).

[63] Ustawa federalna USA z dnia 24 lutego 2016 r. o sądowym zadośćuczynieniu (Judicial Redress Act); 114–126, publikacja 5 U.S.C. § 552a.

[64] Decyzja Rady (UE) nr 2016/2220 z dnia 2 grudnia 2016 r., CELEX: 32016D2220.

[65] Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych, CELEX: 22016A1210(01).

[66] Departament Sprawiedliwości USA, Attorney General Order No. 3824–2017, „Judicial Redress Act of 2015; Attorney General Designations", Federal Register t. 82, nr 13, s. 7860.

[67] Przyczyną nieobjęcia postanowieniami JRA Danii oraz Wielkiej Brytanii jest brak związania obu państw umową parasolową UE–USA, będącego rezultatem możliwości wyłączenia współpracy w sprawach karnych wy-

Należy podkreślić, że Judicial Redress Act nie rozszerza podmiotowo zakresu stosowania Privacy Act, ale tylko nadaje obcokrajowcom określone — nie wszystkie — uprawnienia, z których mogą korzystać obywatele amerykańscy. W szczególności wprowadza możliwość dochodzenia naruszeń przepisów ustawy Privacy Act w postępowaniach cywilnych przed sądami federalnymi. Obywatele UE mogą zatem skorzystać z drogi sądowej w celu uzyskania odszkodowania lub zadośćuczynienia w związku z działaniami władzy publicznej w zakresie przetwarzania ich danych osobowych w sposób niezgodny z Privacy Act.

W tym miejscu należy zwrócić uwagę na istotną różnicę pomiędzy prawem UE a regulacjami wynikającymi z JRA, jaką jest zakres podmiotów uprawnionych. W prawie UE ochrona prywatności oraz danych osobowych przysługuje każdemu, bez ograniczenia wyłącznie do obywateli UE[68]. W rezultacie obywatel państwa trzeciego, którego dane są przetwarzane w związku z działalnością prowadzoną na terenie Unii, może korzystać z praw i gwarancji wynikających z europejskich przepisów o ochronie danych[69]. Także warunki programu „Tarcza prywatności" nie zawężają kręgu podmiotów uprawnionych do osób posiadających obywatelstwo UE[70]. Natomiast ograniczenia takie zostały uwzględnione w ustawie JRA, bowiem zgodnie z przyjętą definicją tzw. uprawnionej osoby (ang. *covered person*) wyłącznie obywatele wskazanych państw i organizacji międzynarodowych mogą korzystać z trybu określonego we wprowadzanych przepisach[71]. W konsekwencji nie każdy podmiot danych uprawniony na mocy przepisów europejskich będzie mógł skorzystać z ochrony sądowej przed sądami amerykańskimi w trybie przewidzianym w JRA.

W ustawie JRA ograniczono także zakres podmiotów zobowiązanych, wprowadzając w tym zakresie pojęcie „wyznaczona agencja" (ang. *designated federal agency*)[72] — tj. agencji rządowej wskazanej w zarządzeniu opublikowanym przez Biuro Prokuratora Generalnego USA. Tylko wyznaczone agencje są zobowiązane do przestrzegania przepisów ustawy Privacy Act w odniesieniu do obcokrajowców, a zatem obywatele UE zyskują możliwość ochrony praw na drodze sądowej jedynie wobec naruszeń będących skutkiem działań wskazanych agencji rządowych. Na aktualnej liście, opublikowanej przez Biuro Prokuratora Generalnego 27 stycznia 2017 r., znajdują się cztery agencje federalne oraz dziewięć biur stanowiących jednostki organizacyjne innych agencji — głównie związanych z kontrolą skarbową

nikających z wynegocjowanych warunków zawarcia traktatów europejskich (por. Protokół 21, art. 6a oraz Protokół 22, art. 2 i 2a TFUE).

[68] W obowiązującym stanie prawnym powszechne rozumienie prawa do prywatności i ochrony danych osobowych nie budzi wątpliwości z uwagi na literalne brzmienie art. 16 TFUE oraz art. 7 i 8 KPP.

[69] Por. rozważania TSUE przedstawione w wyroku w sprawie *Weltimmo*, a związane z przesłankami uzasadniającymi uznanie, że przedsiębiorca prowadzi działalność gospodarczą w kontekście danego państwa członkowskiego UE (C-230/14, pkt 29–41).

[70] Ograniczenia takie — wynikające z decyzji KE — nie mogłyby zostać wprowadzone, ponieważ w sposób oczywisty prowadziłyby do naruszenia przepisów prawa wyższego rzędu (por. przyp. 68).

[71] Zob. art. 2 ust. g pkt 3 JRA.

[72] Zob. art. 2 ust. g pkt 5 JRA.

oraz nadzorem nad rynkiem finansowym. Na liście nie ma Agencji Bezpieczeństwa Narodowego (NSA) ani innych podmiotów realizujących kwestionowane prawnie programy inwigilacji obywateli.

Z uwagi na krótki termin obowiązywania nie ma możliwości oceny praktycznej przydatności JRA do ochrony praw obywateli UE przed sądami federalnymi. Jednak z uwagi na znaczne ograniczenia przedmiotowe i podmiotowe względem praw przysługujących obywatelom i rezydentom USA uzasadniony wydaje się pogląd, że ustawa ta nie wpłynie na wzrost gwarancji dla mieszkańców UE w obszarze ochrony prywatności w związku z przekazaniem ich danych do USA na podstawie programu „Tarcza prywatności".

Kolejne wątpliwości w zakresie znaczenia gwarancji wynikających z „Tarczy prywatności" związane są z dekretem 13768 zatwierdzonym 26 stycznia 2017 r. przez prezydenta D. Trumpa[73]. Głównym celem aktu jest wzmocnienie bezpieczeństwa wewnętrznego poprzez deportację imigrantów nielegalnie przebywających na terenie USA lub naruszających warunki pobytu. Natomiast zgodnie z pkt 14 dekretu nakazano organom władzy wykonawczej podjęcie wszelkich działań mieszczących się w granicach prawa, prowadzących do wyłączenia osób, które nie są obywatelami lub rezydentami USA, z ochrony przewidywanej przez przepisy ustawy Privacy Act.

Analizując znaczenie tego dekretu dla programu „Tarcza prywatności", w pierwszej kolejności należy przypomnieć, że osobami uprawnionymi z ustawy Privacy Act nigdy nie byli obcokrajowcy[74]. W tym znaczeniu dekret prezydenta jest więc wadliwy. Bez wątpienia dekret nie może także wpłynąć na zakres stosowania JRA i uprawnień wynikających z tej ustawy, bowiem zgodnie z amerykańską konstytucją prawo stanowione przez Kongres wiąże władzę wykonawczą[75]. Pogląd ten podzieliła także Komisja Europejska, w specjalnie wydanym oświadczeniu[76].

Jeżeli jednak uznać, że oczekiwaniem głowy państwa było wyłączenie wobec obcokrajowców gwarancji związanych z ochroną danych osobowych przetwarzanych przez administrację publiczną USA, to dekret w dalszej perspektywie może prowadzić do unieważnienia programu „Tarcza prywatności". Należy pamiętać, że program opiera się na zestawie oświadczeń i deklaracji wydanych przez przedstawicieli władzy wykonawczej podległej prezydentowi. Warunki programu nie stanowią części prawa stanowionego, w konsekwencji sam program może zostać jednostron-

[73] Executive Order: Enhancing Public Safety in the Interior of the United States, www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[74] Por. wcześniejsze rozważania dotyczące ustawy Privacy Act.

[75] Dotyczy to sytuacji, w których Konstytucja USA nie przyznaje wprost określonych uprawnień prezydentowi; w takich przypadkach Kongres ma ograniczone możliwości unieważnienia decyzji władzy wykonawczej; więcej: T. Gaziano: *The Use and Abuse of Executive Orders and Other Presidential Directives*, Texas Review of Law & Politics 2000–2001, t. 5, s. 267–303.

[76] P. Bradley-Schmieg, D. Bender: *European Commission Dismisses Privacy Shield Concerns Over Trump Executive Order*, www.insideprivacy.com/international/european-union/european-commission-dismisses-privacy-shield-concerns-over-trump-executive-order/.

nie zmodyfikowany lub zakończony przez stronę amerykańską bez dodatkowych uzgodnień z UE.

Oddzielnym aspektem wymagającym omówienia jest możliwość zmiany lub uchylenia decyzji o adekwatności zabezpieczeń przez KE, a w konsekwencji zakończenia realizacji programu „Tarcza prywatności" przez partnera europejskiego. Chociaż rozpoczęcie stosowania ogólnego rozporządzenia nie będzie stanowiło samoistnej podstawy do unieważnienia lub zmiany decyzji 2016/1250 (zob. wcześniejsze uwagi dotyczące art. 45 ust. 9 rozporządzenia 2016/679), nie można wykluczyć, że w rezultacie okresowego przeglądu sposobu realizacji programu „Tarcza prywatności" Komisja może pozyskać nowe informacje skutkujące koniecznością uznania, że partner amerykański przestał zapewniać odpowiedni stopień ochrony, co z kolei — na podstawie art. 55 ust. 5 rozporządzenia — będzie wiązało się z koniecznością uchylenia, zmiany lub zawieszenia decyzji o adekwatności zabezpieczeń.

Także w decyzji KE 2150/2016 uwzględniono regulacje stanowiące podstawę do przeprowadzania okresowych przeglądów mających na celu wskazanie, czy ustalenia odnośnie do adekwatności stopnia ochrony gwarantowanego przez Stany Zjednoczone w ramach „Tarczy prywatności" są nadal faktycznie i prawnie uzasadnione[77]. Przy czym zgodnie z art. 4 ust. 6 decyzji wystarczająca do wszczęcia przez KE postępowania prowadzącego do zmiany, zawieszenia lub uchylenia aktu może być nie tylko negatywna ocena sposobu realizacji programu „Tarcza prywatności", lecz także przekazanie przez stronę amerykańską niewystarczających wyjaśnień potrzebnych do dokonania oceny.

Pierwsza okresowa ocena funkcjonowania programu „Tarcza prywatności" została przeprowadzona w dniach 18–19 września 2017 r. W przekazanym przez Komisję raporcie podsumowującym czynności audytowe wskazano, że Stany Zjednoczone prawidłowo realizują obowiązki wynikające z warunków realizacji programu[78]. Komisja przedstawiła także stronie amerykańskiej 10 rekomendacji, w których wskazano działania doskonalące, które powinny zostać podjęte w nadchodzącym roku (w tym związane z reformą przepisów o zagranicznych działaniach wywiadowczych[79], powołaniem osoby na stanowisko ombudsmana czy

[77] Zob. motywy 145–149 oraz art. 4 ust. 4 decyzji KE 2016/1250.

[78] Komisja Europejska, *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield*, COM (2017) 611 final, http://ec.europa.eu/newsroom/document.cfm?doc_id=47798, s. 4.

[79] Jednym z ważniejszych obszarów niezgodności pomiędzy prawodawstwem europejskim a amerykańskim jest możliwość i zakres wykorzystywania danych osobowych w tajnych programach inwigilacji prowadzonych przez organy władzy publicznej. W amerykańskim systemie prawnym podstawą do realizacji większości działań tego typu jest ustawa federalna z dnia 25 października 1975 r. o zagranicznych działania wywiadowczych (Foreign Intelligence Surveillance Act, FISA). Akt ten był wielokrotnie nowelizowany w sposób istotnie zmieniający zakres oraz formy dopuszczalnych działań inwigilacyjnych. W związku z faktem, że z dniem 31 grudnia 2017 r. utraciła moc część z przepisów szczegółowych ustawy FISA, w Stanach Zjednoczonych trwa ożywiona debata publiczna na temat zasadności utrzymania obecnych rozwiązań prawnych w mocy. Rekomendacja KE wpisuje się w tę dys-

wprowadzeniem przez Departament Handlu USA cyklicznych audytów zgodności z warunkami programu)[80].

6. PODSUMOWANIE

„Zagrożenie terroryzmem i rozwój przestępczości zorganizowanej powodują, że coraz częściej musimy godzić się na takie działania służb chroniących porządek prawny i nasze bezpieczeństwo, które ograniczają swobody obywatelskie, w tym sferę prywatności"[81].

Ta teza Naczelnego Sądu Administracyjnego bez wątpienia odzwierciedla problem prawny leżący u podstaw współpracy transatlantyckiej UE–USA w obszarze przetwarzania danych osobowych. Dyskusja związana z odmiennymi wagami przykładanymi w krajowych porządkach różnym prawom podstawowym, a w szczególności prawu do wolności i bezpieczeństwa osobistego, często wiązanego z obszarem bezpieczeństwa narodowego, oraz prawu do poszanowania prywatności, znalazła odzwierciedlenie w wątpliwościach dotyczących skuteczności programu „Tarcza prywatności".

Działania agencji rządowych USA, prowadzące do naruszenia konstytucyjnych praw i gwarancji wynikających z Karty praw podstawowych UE, doprowadziły nie tylko do unieważnienia umowy „Bezpieczna przystań", lecz także do podważenia zaufania do partnera amerykańskiego w dalszych rozmowach związanych z transatlantyckim przepływem danych.

Bez wątpienia „Tarcza prywatności" wprowadza wiele nowych mechanizmów, które mogą się przyczynić do zwiększenia zaufania mieszkańców UE związanego z ochroną ich informacji przekazywanych do amerykańskich podmiotów. Wydaje się jednak, że zaproponowane rozwiązania — takie jak rozbudowany model arbitrażu czy wprowadzenie możliwości dochodzenia praw przed sądami federalnymi — nie będą miały realnej skuteczności z uwagi na wewnętrzny system prawny USA. Nawet wprowadzenie ustawy Judicial Redress Act nie zmienia tej oceny, ponieważ prowadzi do nadania obywatelom UE tylko fragmentu uprawnień przynależnych obywatelom i rezydentom USA na podstawie i tak bardzo ograniczonych przepisów Privacy Act. Nie bez przyczyny w literaturze przedmiotu wskazuje się, że aby obywatele UE posiadali na gruncie prawa USA podobne gwarancje związane z posza-

kusję, jednakże *de facto* dotyczy działań przyszłych prawodawcy amerykańskiego, nie ma więc bezpośredniego związku z oceną realizacji programu „Tarcza prywatności" w badanym okresie.

[80] Szczegółowe omówienie rekomendacji: *Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield — Commission Staff Working Document*, Bruksela 18.20.2017, SWD(2017) 344 final. http://ec.europa.eu/newsroom/document.cfm?doc_id=47799.

[81] Wyrok NSA z dnia 28 kwietnia 2016 r., I OSK 2620/14, Legalis nr 1510118.

nowaniem prywatności co w prawodawstwie unijnym, przepisy federalne powinny nadawać im większe prawa i uprawnienia niż obywatelom USA[82].

Utworzenie programu „Tarcza prywatności" wyłącznie w oparciu o deklaracje i oświadczenia urzędników rządu USA, bez dodatkowych gwarancji wynikających na przykład z nadania warunkom programu statusu umowy międzynarodowej, powoduje, że istnieje poważne ryzyko jednostronnej zmiany warunków programu, oraz zwiększa ryzyko braku trwałości uzgodnień na skutek zmiany polityki ze strony nowej administracji USA. Obecnie możliwość realizacji programów inwigilacji obywateli w oparciu o hurtowe i nieukierunkowane przetwarzanie danych jest ograniczona głównie na podstawie decyzji władzy wykonawczej, a nie przepisów prawa federalnego. Najważniejsza w tym zakresie dyrektywa polityczna prezydenta nr 28[83] (Presidential Policy Directive 28, PPD-28), przywoływana także wielokrotnie w oświadczeniach urzędników USA[84] stanowiących załącznik do decyzji KE ustanawiającej program „Tarcza prywatności", została wydana przez prezydenta B. Obamę i może zostać łatwo zmieniona lub unieważniona przez obecną administrację.

Wątpliwości co do zgodności „Tarczy prywatności" z prawem UE, wyrażane w niniejszym artykule oraz szeroko omawiane w literaturze przedmiotu, mogą doprowadzić do unieważnienia przez TSUE decyzji KE 2016/1250, stanowiącej podstawę dla realizacji „Tarczy prywatności". Należy przypomnieć, że w wyroku w sprawie *Schrems* Trybunał jasno wskazał procedurę postępowania, która powinna być wykorzystana do zakwestionowania ważności istniejących oraz przyszłych decyzji o adekwatności wydanych przez Komisję Europejską. Już we wrześniu 2016 r. organizacja Digital Rights Ireland (DRI) wniosła do Trybunału Sprawiedliwości UE skargę mającą na celu stwierdzenie nieważności decyzji KE 2016/1250[85]. W swojej skardze DRI podnosi dziesięć zarzutów dowodzących, jej zdaniem, że Komisja Europejska dopuściła się błędu w ocenie stanu faktycznego, w zakresie, w jakim uznała Stany Zjednoczone za państwo zapewniające odpowiedni stopień ochrony danych osobowych, zgodny z dyrektywą 95/46.

Niezależnie od zakończenia postępowania ze skargi DRI oraz ewentualnie innych działań prawnych mających wpływ na stosowanie „Tarczy prywatności"[86],

[82] D. Bender: *The Judicial Redress Act: A Path To Nowhere*, http://cli.re/Ger32o.

[83] Prezydencka Dyrektywa Polityczna nr 28 (PPD-28) dotycząca aktywności w obszarze wywiadu elektronicznego (ang. *signal intelligence*), 17 stycznia 2014 r., http://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities-0.

[84] Zob. np. motyw 94 decyzji 2016/1250; pismo amerykańskiego Sekretarza Stanu (zał. III); oświadczenie Rzecznika ds. „Tarczy prywatności" UE-USA (zał. A do zał. 3), pismo Urzędu Dyrektora Krajowych Służb Wywiadowczych (zał. VI).

[85] Skarga do TSUE, sprawa *Digital Rights Ireland v. Komisja Europejska*, T-670/16.

[86] Wymienić należy m.in. sprawę *Microsoft v. Stany Zjednoczone* (829 F.3d 197 2016), dotyczącą zobowiązania Microsoft Corp. (spółka prawa amerykańskiego) do wydania kopii danych składowanych w centrum przetwarzania w Irlandii i zarządzanych przez podmiot zależny Microsoft (spółkę prawa irlandzkiego). Wydanie prawomocnego orzeczenia zobowiązującego Microsoft do przekazania kopii danych prowadziłoby do faktycznego

jako wniosek *de lege ferenda* zasadne wydaje się przyjęcie, aby przyszłe decyzje o adekwatności wydawane przez Komisję Europejską bazowały wprost na ocenie prawa materialnego stosowanego w państwie trzecim, a nie zmierzały do uznania jako wystarczającego istnienia quasi-prawnych mechanizmów niewywodzących się z prawa stanowionego. Tylko w takim przypadku prawa jednostki, stanowiące fundament funkcjonowania Unii, będą mogły być w pełni chronione w sposób zgodny z postanowieniami Karty praw podstawowych UE.

BIBLIOGRAFIA

Barta J., Fajgielski P., Markiewicz R.: *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

Bender D.: *The Judicial Redress Act: A Path To Nowhere*, http://cli.re/Ger32o.

Cole D.: *Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens?*, Thomas Jefferson Law Review 2003, t. 25, s. 367–388.

Fischer B., Karwala D.: *Transfer danych osobowych do państw trzecich*, Państwo i Prawo 2007, z. 1, s. 100–112.

Garcia M.: *International Law and Agreements — Their Effect upon U.S. Law*, Congressional Research Service 2015, http://cli.re/LvbD1M.

Gaziano T.: *The Use and Abuse of Executive Orders and Other Presidential Directives*, Texas Review of Law & Politics 2000–2001, t. 5, s. 267–303.

Gold A.: *Obscured by clouds: the Fourth Amendment and searching cloud storage accounts through locally installed software*, William & Mary Law Review 2015, nr 6, s. 2321–2350.

Jagielska M., Kunkiel-Kryńska A.: *Wybór prawa jako klauzula abuzywna w umowach konsumenckich zawieranych przez Internet*, IKAR 2016, nr 3, s. 29–38.

Jaroszek A.: *Ważność wyboru* (w:) A. Jaroszek: *Prawo właściwe dla umów konsumenckich zawieranych przez Internet*, Warszawa 2009.

Johnson E.: *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, Stanford Law Review 2017, t. 69, s. 867–909.

Kerr O.: *The Fourth Amendment in cyberspace: can encryption create a resonable expectation of privacy?*, Connecticut Law Review 2001, t. 33, s. 503–533.

Kolasiński M., Świerczyński M.: *Wybór prawa obcego w internetowych wzorcach umownych — obowiązek spojrzenia na ochronę konsumentów z perspektywy prawa prywatnego międzynarodowego* (w:) *Prawo konsumenckie w praktyce*, pod red. M. Czarneckiej, T. Skocznego, Warszawa 2016, s. 19–30.

transgranicznego przepływu informacji z pominięciem przepisów prawa UE. Szersze omówienie sprawy: M. Rojszczak: *Ochrona tajemnicy…*, *op. cit.*, s. 170–171.

Krzysztofek M.: *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016.

Motyka K.: *Prawo do prywatności*, Zeszyty Naukowe Akademii Podlaskiej w Siedlcach, Seria Administracja i Zarządzanie 2010, nr 85, s. 9–36.

Shaffer G.: *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Data Privacy Standards*, Yale Journal of International Law 2000, nr 1, s. 1–87.

Solove D.: *The Scope and Potential of FTC Data Protection*, The George Washington Law Review 2015, nr 6, s. 2230–2300.

MARCIN ROJSZCZAK

EFFECTIVENESS OF THE PROTECTION OF THE DATA SUBJECT'S RIGHTS GUARANTEED IN EU LAW IN THE CONTEXT OF THE PRIVACY SHIELD AGREEMENT AND THE US FEDERAL LAWS

S u m m a r y

The purpose of this article is to discuss recent developments in the EU–US relations related to the protection of personal data. The Privacy Shield Agreement negotiated in 2016 has resulted in the resumption of the EU–US cross-border flow of data suspended following the CJEU judgment in the Schrems case. The Court in its ruling pointed to the fundamental problems of the incompatibility of the EU and US legislation, in particular in the area of protection of basic values guaranteed by the EU Charter of Fundamental Rights. Implementation of the General Data Protection Regulation is also important factor in discussion of existing and future EU–US data flows regulations.

Comparison between Privacy Shield and its predecessor — the Safe Harbor– is used to reveal important improvements that were implemented to ensure compatibility with the EU regulations. This includes updated set of rules that US organizations should follow when processing data transferred from EU. In result, regulations related to transatlantic cooperation in the area of protection of privacy and personal data require a deeper analysis not only on the grounds of existing judgments of the CJEU, but also in the light of the US legal safeguards that are available to data subjects. One of the new US legal mechanisms that is intended to provide adequate guarantees of protection for EU individuals relates to the Judicial Redress Act. Several aspects of this new legislation are analyzed in the article and its findings may indicate that „adequate" protection, i.e. one of the fundamental requirement under EU law and Privacy Shield program, may in fact not be provided.

Another aspect of analysis is related to the change of policy of limiting the priority of national security programs, including electronic surveillance, made by the current US administration, which also may affects UE–US agreements related to data protection area.

In the final conclusions, recommendation regarding existing and future cross-border data flows agreements are formulated.