16/PL
WP 238

Opinia nr 1/2016 dotycząca projektu decyzji stwierdzającej odpowiedni stopień ochrony w ramach Tarczy Prywatności UE-USA

Przyjęta w dniu 13 kwietnia 2016 r.

STRESZCZENIE

29 lutego 2016 r. Komisja Europejska opublikowała komunikat, projekt decyzji w sprawie odpowiedniej ochrony danych osobowych oraz załączone do niego teksty, stanowiące nowe ramy transatlantyckiej wymiany danych osobowych do celów handlowych: Tarcza Prywatności UE-USA (zwana dalej Tarczą Prywatności), której zadaniem jest zastąpienie obowiązującego wcześniej programu USA „bezpieczna przystań", unieważnionego przez Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE) w dniu 6 października 2015 r. w sprawie Schrems.

Zgodnie z art. 30 ust. 1 lit. c) dyrektywy 95/46/WE Grupa Robocza Art. 29 (zwana dalej: WP29) przeanalizowała te dokumenty w celu wyrażenia swojej opinii na temat projektu decyzji w sprawie odpowiedniej ochrony danych osobowych. WP29 przeanalizowała zarówno aspekty handlowe jak i potencjalne odstępstwa od zasad Tarczy Prywatności na potrzeby bezpieczeństwa narodowego, egzekwowania prawa i interesu publicznego.

WP29 uwzględniła mające zastosowanie ramy prawne UE dotyczące ochrony danych opisane w dyrektywie 95/46/WE, a także prawa podstawowe dotyczące życia prywatnego i ochrony danych zawarte w art. 8 Europejskiej konwencji praw człowieka, a także w art. 7 i art. 8 Karty praw podstawowych Unii Europejskiej. Uwzględniła także prawo do skutecznego środka prawnego oraz dostępu do bezstronnego sądu wskazane w art. 47 Karty, a także orzecznictwo w zakresie poszczególnych praw podstawowych.

Dodatkowo analiza odzwierciedla argumentację TSUE w sprawie Schrems dotyczącą marginesu swobody Komisji w zakresie oceny odpowiedniego stopnia ochrony danych osobowych. Bezwzględnie realizowane muszą być środki kontroli dotyczące wymagań w sprawie odpowiedniej ochrony, z uwzględnieniem praw podstawowych do prywatności, ochrony danych oraz liczby osób, na które przekazywanie danych może mieć potencjalny wpływ.

Tarczę Prywatności postrzegać należy w bieżącym kontekście międzynarodowym, także w związku z pojawieniem się technologii dużych zbiorów danych i rosnącymi potrzebami w zakresie bezpieczeństwa. Zakres zbierania i wykorzystywania danych osobowych znacząco wzrósł od czasu wydania pierwszej decyzji w sprawie programu „bezpieczna przystań" w 2000 r. Europejskie organy ochrony danych zdecydowanie podkreślają wagę zasad, których strzegą.

WP29 przede wszystkim z zadowoleniem przyjmuje znaczącą poprawę, jaką niesie ze sobą Tarcza Prywatności w porównaniu do decyzji w sprawie programu „bezpieczna przystań" WP29 odnotowała, że negocjatorzy pracowali nad wieloma niedociągnięciami programu „bezpieczna przystań", które Grupa przedstawiła w swoim piśmie z dnia 10 kwietnia 2014 r. do wiceprzewodniczącej Reding.

Fakt, że zasady i gwarancje ustanawiane na mocy Tarczy Prywatności są zawarte zarówno w decyzji stwierdzającej odpowiedni stopień ochrony, jak i w załącznikach do niej, sprawia, że

informacje te trudno jest odnaleźć, a czasem również są one niespójne. Przyczynia się to do ogólnego braku czytelności nowych ram, a także utrudnia dostęp ze strony osób, których dane dotyczą, podmiotów, a także organów ochrony danych. Są one również sformułowane w niezrozumiałym dla użytkownika języku. WP29 w związku z tym wzywa Komisję do tego, by uczyniła tekst czytelnym i zrozumiałym po obu stronach Atlantyku.

W odniesieniu do obowiązującego prawa WP29 podkreśla, że jeżeli na podstawie dyrektywy 95/46/WE przyjęta zostanie decyzja w sprawie odpowiedniej ochrony danych osobowych, będzie ona musiała być spójna z ramami prawnymi ochrony danych w UE, zarówno pod względem zakresu, jak i terminologii. WP29 uważa, że wkrótce po wejściu w życie ogólnego rozporządzenia w sprawie ochrony danych należy przeprowadzić przegląd w celu zapewnienia, że wyższy poziom ochrony danych, jaki oferuje to rozporządzenie, został uwzględniony w decyzji w sprawie odpowiedniej ochrony danych osobowych i w załącznikach do niej.

Aspekty handlowe Tarczy Prywatności

Kluczowym celem WP29 jest zapewnienie, aby podczas przetwarzania danych na podstawie postanowień Tarczy Prywatności utrzymany został co do zasady równoważny poziom ochrony danych osób fizycznych. WP29 nie spodziewa się, że Tarcza Prywatności będzie dokładną i wyczerpującą kopią ram prawnych UE, jednak uważa, że powinna odpowiadać treści fundamentalnych zasad w tym zakresie i tym samym zapewniać „co do zasady równoważny" poziom ochrony.

Niezależnie od ulepszeń występujących w Tarczy Prywatności WP29 uważa, że niektóre kluczowe zasady ochrony danych występujące w prawie europejskim nie znalazły się w projekcie decyzji w sprawie odpowiedniej ochrony danych osobowych i załącznikach do niej, lub zostały nieodpowiednio zastąpione przez koncepcje alternatywne.

Na przykład z obecnego brzmienia zasady celowości i integralności danych nie można jednoznacznie wyprowadzić zasady przechowywania danych ani nie została ona wyraźnie wymieniona. Dodatkowo brak jest wzmianki dotyczącej ochrony, która powinna objąć automatyczne, indywidualne decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu. Zastosowanie zasady celowości do przetwarzania danych również jest niejasne. W celu wprowadzenia większej przejrzystości w odniesieniu do stosowania pewnych istotnych koncepcji WP29 sugeruje uzgodnienie między UE a USA jednoznacznych definicji terminów, i umieszczenie ich w glosariuszu stanowiącym część najczęściej zadawanych pytań w sprawie Tarczy Prywatności.

Ponieważ Tarcza Prywatności będzie także wykorzystywana do przekazywania danych poza terytorium USA, WP29 podkreśla, że dalsze przekazywanie przez podmiot objęty Tarczą Prywatności do odbiorcy z państwa trzeciego powinno zapewniać ten sam poziom ochrony w zakresie wszystkich aspektów Tarczy (w tym bezpieczeństwa narodowego) i nie powinno prowadzić do poluzowania lub obejścia zasad ochrony danych w UE. Na wypadek, gdyby Tarcza Prywatności przewidywała dalsze przekazywanie danych do państwa trzeciego, każda

podmiot uczestniczący w Tarczy Prywatności powinien zostać zobowiązany – przed przekazaniem danych – do oceny obowiązujących przepisów państwa trzeciego mających zastosowanie do importera danych. Ogólnie rzecz biorąc WP29 stwierdza, że przedmiot dalszego przekazywania danych osobowych z UE nie został wystarczająco omówiony przede wszystkim jeśli chodzi o jego zakres, zasadę celowości i gwarancje dotyczące przekazywania danych przedstawicielom.

Wreszcie– chociaż WP29 odnotowała udostępnienie dodatkowych środków egzekwowania swoich praw osobom fizycznym, obawia się, że nowy mechanizm dochodzenia roszczeń może w praktyce okazać się zbyt złożony, trudny do wykorzystania dla osób fizycznych z UE i tym samym nieskuteczny. W związku z tym wymagane są dalsze wyjaśnienia dotyczące poszczególnych procedur odwoławczych. W szczególności, w przypadku wyrażenia przez nie zgody, punktami kontaktowymi dla obywateli UE mogłyby być w ramach różnych procedur organy ochrony danych UE, które miałyby możliwość działania w imieniu unijnych obywateli.

Odstępstwa ze względu na kwestie bezpieczeństwa narodowego

W odniesieniu do dostępu organów publicznych do danych zarówno w UE, jak i w państwach trzecich, WP29 przypomina o swojej analizie stosownych praw podstawowych, zawartej w dokumencie roboczym w sprawie uzasadnienia ingerencji w prawa podstawowe do prywatności i ochrony danych za pomocą środków nadzoru podczas przekazywania danych osobowych (zasadnicze gwarancje europejskie) (WP237).

Dużym krokiem naprzód od momentu wydania decyzji dotyczącej programu bezpiecznej przystani jest fakt, że obecny projekt decyzji w sprawie odpowiedniej ochrony danych osobowych w dużej mierze dotyczy możliwego dostępu do danych przetwarzanych na podstawie Tarczy Prywatności na potrzeby bezpieczeństwa narodowego i egzekwowania prawa. WP29 docenia ten znaczący krok, a także większą przejrzystość oferowaną przez władze USA w zakresie przepisów dotyczących zbierania danych do celów wywiadowczych (załącznik VI).

WP29 zwraca jednak uwagę, że oświadczenia amerykańskiego Urzędu Dyrektora Krajowych Służb Wywiadowczych (ODNI) nie wykluczają masowego i nieróżnicowanego zbierania danych osobowych pochodzących z UE. WP29 przypomina o swym dawno ugruntowanym stanowisku, że masowe i nieróżnicowane inwigilowanie jednostek nigdy nie może być uznane za proporcjonalne i nieodzownie konieczne w społeczeństwie demokratycznym, czego wymaga stopień ochrony, jaki dają stosowne prawa podstawowe. Dodatkowo kluczowe znaczenie ma kompleksowy nadzór nad wszystkimi programami inwigilacji. WP29 zwraca uwagę na fakt, że w świetle walki z terroryzmem istnieje tendencja do bezkrytycznego zbierania coraz większej ilości danych na masową skalę. Biorąc pod uwagę wątpliwości, jakie wzbudza ten fakt w kontekście ochrony praw podstawowych do prywatności i ochrony danych, WP29 liczy na korzystne orzeczenia TSUE w sprawach dotyczących masowego i nieróżnicowanego zbierania danych.

W zakresie dochodzenia roszczeń WP29 z zadowoleniem przyjmuje powołanie rzecznika jako nowego środka odwoławczego, ale uważa, że ta nowa instytucja nie jest wystarczająco niezależna ani wyposażona w odpowiednie uprawnienia do rzeczywistego sprawowania swoich obowiązków oraz nie gwarantuje zadowalającego środka odwoławczego w razie braku porozumienia.

Wspólny przegląd

Mechanizm corocznego wspólnego przeglądu, o którym mowa w projekcie decyzji w sprawie odpowiedniej ochrony danych osobowych, stanowi kluczowy element ogólnej wiarygodności Tarczy Prywatności, a WP29 z wielkim zadowoleniem przyjmuje ewentualną możliwość przeglądu decyzji w sprawie odpowiedniej ochrony danych osobowych. WP29 zakłada, że krajowi przedstawiciele WP29 będą mogli w pełni uczestniczyć procesie przeglądu, ale prosi o wyjaśnienia dotyczące szczegółowych uzgodnień w tym zakresie. Wszystkie możliwe opcje (w tym ostateczne sprawozdanie, jego publikacja i potencjalne skutki, a także finansowanie) należy uzgodnić odpowiednio wcześniej przed przeprowadzeniem pierwszego przeglądu.

Wnioski

WP29 zauważa znaczące ulepszenia w Tarczy Prywatności w porównaniu do unieważnionej decyzji w sprawie programu „bezpieczna przystań". Biorąc pod uwagę wyrażone wątpliwości i prośbę o przedstawienie wyjaśnień, WP29 wzywa komisję do eliminacji tych obaw, określenia odpowiednich rozwiązań i przekazania wspominanych wyjaśnień w celu poprawy projektu decyzji w sprawie odpowiedniej ochrony danych osobowych i zagwarantowania, że ochrona oferowana przez Tarczę Prywatności rzeczywiście jest co do zasady równoważna względem ochrony w UE.

SPIS TREŚCI

1. WPROWADZENIE

Po wyroku wydanym przez Trybunał Sprawiedliwości Unii Europejskiej (zwany dalej: TSUE) dnia 6 października 2015 r. w sprawie Schrems[1] Grupa Robocza Art. 29 (zwana dalej: WP29 lub Grupą Roboczą) zaapelowała do państw członkowskich Unii Europejskiej (zwanej dalej: UE) i pozostałych instytucji europejskich o rozpoczęcie rozmów z władzami Stanów Zjednoczonych (zwanymi dalej: USA) w celu znalezienia rozwiązań politycznych, prawnych i technicznych umożliwiających przekazywanie danych na terytorium USA z poszanowaniem praw podstawowych.

2 lutego 2016 r., po ponad dwóch latach negocjacji, Komisja Europejska i amerykański Departament Handlu (DoC) osiągnęły polityczne porozumienie w sprawie *Nowych ram transatlantyckiej wymiany danych osobowych do celów handlowych: Tarcza Prywatności UE-USA* (zwana dalej: (Tarczą Prywatności), której celem jest zastąpienie obowiązującego uprzednio amerykańskiego programu bezpiecznej przystani.

29 lutego 2016 r. Komisja opublikowała komunikat[2] - projekt decyzji w sprawie odpowiedniej ochrony danych osobowych oraz załączone do niego teksty, które stanowią Tarczę Prywatności. Zgodnie z art. 30 ust. 1 lit. c) dyrektywy 95/46/WE (zwanej dalej: Dyrektywą) WP29 przeanalizowała te dokumenty w celu przedstawienia swojej aktualnej opinii w sprawie projektu decyzji stwierdzającej odpowiedni stopień ochrony przygotowanej przez Komisję, w tym w sprawie stanowiących jej podstawę dokumentów Tarczy Prywatności. W ramach oceny WP29 podzieliła prace na analizę handlowej części Tarczy Prywatności i analizę gwarancji wdrożonych w zakresie odstępstw od zasad Tarczy Prywatności na potrzeby bezpieczeństwa narodowego, egzekwowania prawa i interesu publicznego.

Po wyroku w sprawie Schrems WP29 odbyła szereg spotkań z delegacjami amerykańskich władz, przedstawicielami organizacji społeczeństwa obywatelskiego z UE i USA oraz naukowcami w celu przygotowania oceny skutków wyroku w sprawie Schrems. W trakcie oceny Tarczy Prywatności odbyły się dodatkowe spotkania z Komisją Europejską i przedstawicielami władz USA. W ramach tych spotkań przekazano pewne wyjaśnienia, które także zostały uwzględnione w niniejszej opinii. WP29 podkreśla, że na tym etapie wyjaśnienia te miały jedynie charakter nieoficjalny i nie można uważać, że stanowią integralną część projektu decyzji w sprawie odpowiedniej ochrony danych osobowych, ponieważ nie zostały one złożone na piśmie.

Niezależnie od tego WP29 ze szczególnym zadowoleniem przyjmuje podjęte przez DoC podczas tych rozmów zobowiązanie do współpracy z organami ochrony danych państw członkowskich w zakresie stosowania Tarczy Prywatności, a także sporządzenia wskazówek i interpretacji prawnej dotyczącej zastosowania Tarczy Prywatności, które zostaną opublikowane na ich stronach internetowych.

[1] Sprawa C-362/14 - Maximilian Schrems przeciwko Data Protection Commissioner, 6 października 2015 r. (zwana dalej: Schrems)
[2] COM (2016)117 final, 29 lutego 2016 r.

1.1 Uwagi ogólne

1.1.1 Zakres oceny WP29

WP29 przede wszystkim uwzględniła obowiązujące w państwach członkowskich Unii Europejskiej ramy ochrony danych, w tym art. 8 Europejskiej konwencji praw człowieka (zwanej dalej: ECHR) chroniący prawo do życia prywatnego i rodzinnego, a także art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej: Kartą) chroniące, odpowiednio, prawo do życia prywatnego i rodzinnego, prawo do ochrony danych osobowych, a także prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu. Grupa Robocza uwzględniła także orzecznictwo w tej dziedzinie, a także wymagania Dyrektywy.

TSUE w sprawie Schrems dodatkowo zdefiniował wymóg obowiązujący wobec państwa trzeciego, a dotyczący zapewnienia wystarczającego stopnia ochrony danych. Trybunał nie tylko wyjaśnił, że postanowienia Dyrektywy muszą być interpretowane „w świetle praw podstawowych gwarantowanych przez Kartę”[3], a w szczególności art. 7 i art. 8. Wskazał on także, że wyrażenie „odpowiedni stopień ochrony” należy rozumieć jako „wymagające od tego państwa trzeciego skutecznego zapewnienia, ze względu na jego ustawodawstwo wewnętrzne lub zobowiązania międzynarodowe, poziomu ochrony podstawowych praw i wolności merytorycznie równoważnego poziomowi gwarantowanemu w Unii na mocy dyrektywy w związku z kartą”[4]. Dla obowiązującej uprzednio decyzji w sprawie programu „bezpieczna przystań” taka ocena nigdy nie została przeprowadzona na odpowiednim poziomie szczegółowości. WP29 w związku z tym przeprowadziła ocenę projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w świetle wymogu zapewnienia analizy poziomu ochrony praw i wolności podstawowych, który musi być *zasadniczo równoważny* względem gwarantowanego na terenie UE. WP29 podkreśla, że w niniejszej opinii zawarto jej podstawowe wątpliwości, jednak biorąc pod uwagę krótki czas, jaki minął od publikacji projektu decyzji w sprawie odpowiedniej ochrony danych osobowych, w późniejszym terminie zidentyfikowane mogą być inne problemy.

WP29 przyjmuje do wiadomości, że definiując wyrażenie „odpowiedni” w art. 25 ust. 6 Dyrektywy jako „merytorycznie równoważny”, TSUE dodatkowo objaśnił tę równoważność w sprawie Schrems. Trybunał podkreślił, że wyrażenie „odpowiedni stopień ochrony”, mimo tego, że nie wymaga od państwa trzeciego zapewnienia stopnia ochrony identycznego do stopnia gwarantowanego w porządku prawnym UE należy rozumieć jako co do zasady wymagające od państwa trzeciego, poprzez jego prawo krajowe lub zobowiązania międzynarodowe, poziomu ochrony praw i wolności podstawowych, który jest *merytorycznie równoważny* poziomowi ochrony gwarantowanemu w Unii Europejskiej na mocy dyrektywy odczytywanej w kontekście Karty.

[3] Schrems, pkt 38
[4] Schrems, pkt 73

1.1.2 Ocena części handlowej projektu decyzji w sprawie odpowiedniej ochrony danych osobowych

WP29 wyjaśniła już sposób, w jaki zastosowała główne zasady ochrony danych w UE wobec przekazywania danych osobowych do państw trzecich w swoim dokumencie roboczym nr 12 „Przekazywanie danych osobowych do państw trzecich: stosowanie art. 25 i 26 dyrektywy UE o ochronie danych”[5]. WP29 starała się odnaleźć równoważne gwarancje, które zapewniają stopień ochrony odpowiadający zasadom gwarantowanym w Dyrektywie, w szczególności w zakresie celowości, jakości danych oraz proporcjonalności, przejrzystości, bezpieczeństwa, prawa do dostępu, sprostowania i sprzeciwu, przechowywania danych i ograniczeń w ich dalszym przekazywaniu. Podobną metodę zastosowano w opiniach wydanych przez WP29 w trakcie oceny pierwotnej decyzji w sprawie odpowiedniej ochrony danych osobowych programu „bezpieczna przystań”[6], a także w zaleceniach sformułowanych przez Grupę Roboczą w jej piśmie do byłej wiceprzewodniczącej i komisarz UE ds. sprawiedliwości Viviane Reding, opublikowanym dnia 10 kwietnia 2014 r.[7]

1.1.3 Ocena odstępstw w zakresie dostępu organów publicznych i ich gwarancje

Ocena odstępstw w zakresie dostępu organów publicznych do danych osobowych na podstawie Tarczy Prywatności to problem złożony, w szczególności przy uwzględnieniu większej świadomości organów ochrony danych oraz opinii publicznej na temat programów inwigilacji przez USA po doniesieniach Snowdena. Grupa Robocza z zadowoleniem przyjmuje do wiadomości wysiłki władz USA na rzecz zwiększenia przejrzystości w odniesieniu do programów inwigilacji i chęć uwzględnienia w Tarczy Prywatności dodatkowych gwarancji. Jednocześnie WP29 podkreśla, że jakakolwiek ingerencja w prawa podstawowe do życia prywatnego i ochrony danych musi posiadać uzasadnienie w społeczeństwie demokratycznym. TSUE skrytykował fakt, że decyzja w sprawie programu „bezpieczna przystań” nie zawierała żadnych ustaleń dotyczących istnienia w Stanach Zjednoczonych zasad przyjętych na poziomie państwowym, których celem byłoby ograniczenie takiej ingerencji. Brak jest tam również wzmianki o skutecznej ochronie prawnej przed ingerencjami tego typu.[8]

W związku z powyższym WP29 przeanalizowała obecne ramy prawne USA i praktyki amerykańskich agencji wywiadowczych opisane w załącznikach do projektu decyzji, a także warunki, na podstawie których umożliwiają one jakąkolwiek ingerencję w prawa podstawowe do życia prywatnego i ochrony danych, które chronione są na mocy europejskich ram prawnych.

W celu oceny, czy naruszenia takie miałyby uzasadnienie w społeczeństwie demokratycznym, ocenę przeprowadzono w kontekście europejskiego orzecznictwa w dziedzinie praw

[5] Przyjęte przez WP29 dnia 24 lipca 1998 r., zob. w szczególności s. 6.
[6] Zob. WP62, WP32, WP27, WP23, WP21, WP19, WP15 oraz WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems, pkt 87 i 88.

podstawowych, które ustanawia cztery zasadnicze gwarancje[9] dotyczące czynności wywiadowczych:

A. Przetwarzanie danych powinno mieć miejsce zgodnie z prawem i w oparciu o czytelne, precyzyjne i dostępne zasady: oznacza to, że każda osoba posiadająca rozsądny poziom wiedzy powinna być w stanie przewidzieć co stanie się z jej danymi po ich przekazaniu.
B. Należy wykazać konieczność i proporcjonalność w odniesieniu do realizowanych uzasadnionych prawem celów; należy znaleźć równowagę pomiędzy celem, dla którego dane są zbierane i udostępniane, a prawami jednostki.
C. Powinien istnieć niezależny mechanizm kontroli o skutecznym i bezstronnym charakterze: może być to sędzia lub inny niezależny organ, o ile posiada wystarczającą zdolność do przeprowadzania odpowiednich kontroli.
D. Osoby fizyczne powinny mieć dostęp do skutecznych środków prawnych: każdy powinien mieć prawo do obrony swoich praw przed niezależnym organem.

1.2 Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych

WP29 przede wszystkim z zadowoleniem przyjmuje fakt, że w okresie krótszym niż sześć miesięcy po tym, jak TSUE uznał decyzję w sprawie programu „bezpieczna przystań" za nieważną, można wszcząć nową procedurę w sprawie odpowiedniej ochrony danych osobowych. Biorąc pod uwagę ilość codziennie przekazywanych danych pomiędzy UE a USA, co według WP29 stanowi ważną część gospodarek po obu stronach Atlantyku, jasność prawa w tym względzie potrzebna jest raczej wcześniej niż później.

WP29 żałuje przy tym, że projekt decyzji w sprawie odpowiedniej ochrony danych osobowych opublikowany przez Komisję nie zawiera kompleksowej analizy prawa krajowego i międzynarodowych zobowiązań USA w formie sprawozdania dotyczącego odpowiedniej ochrony danych osobowych, co było regularną praktyką w przeszłości w podobnych postępowaniach i jest zgodne z art. 25 Dyrektywy. Uniemożliwiło to WP29 przeprowadzenie pełnej analizy kontekstu prawnego, w którym funkcjonować będzie Tarcza Prywatności. WP29 zwraca na przykład uwagę, że obecny projekt decyzji w sprawie odpowiedniej ochrony danych osobowych nie zawiera ustaleń dotyczących przepisów w zakresie prywatności i ochrony danych obowiązujących w USA, ani na szczeblu federalnym, ani stanowym, w tym przepisów sektorowych czy przepisów dopuszczających formy dostępu organów publicznych niezwiązanego z inwigilacją. Nie jest także zdefiniowana relacja pomiędzy przekazywaniem danych na podstawie Tarczy Prywatności a ich przekazywaniem na podstawie innych istniejących uzgodnień w zakresie odpowiedniego stopnia ochrony takich jak umowa UE-USA w sprawie danych dotyczących przelotu pasażera (PNR) oraz w ramach umowy dotyczącej Programu śledzenia środków finansowych należących do terrorystów (TFTP).

[9] Europejskie Gwarancje Podstawowe wynikają z orzecznictwa TSUE i Europejskiego Trybunału Praw Człowieka; bardziej szczegółowo omówiono je w Dokumencie Roboczym WP237 Grupy Roboczej WP29, opublikowanym 13 kwietnia 2016 r.

1.2.1 Zakres zastosowania ram ochrony danych UE, a w szczególności zasad zawartych w dyrektywie 95/46/WE

WP29 przypomina, że na podstawie ram prawnych UE w sprawie ochrony danych, a w szczególności na podstawie Dyrektywy (art. 4 ust. 1), przepisy państw członkowskich obowiązują nie tylko względem czynności przetwarzania realizowanych przez administratorów danych prowadzących działalność na ich terytorium, lecz także wtedy, gdy administratorzy danych (którzy nie prowadzą działalności na terenie UE) wykorzystują urządzenia znajdujące się na terytorium Unii Europejskiej, w szczególności do zbierania danych osobowych. Skutkiem tego prawo państwa członkowskiego UE dotyczy każdego przypadku przetwarzania, który ma miejsce przed przekazaniem danych do USA, albo w kontekście czynności podmiotu prowadzącego działalność w UE lub za pośrednictwem urządzeń znajdujących się w UE i wykorzystywanych przez podmiot, który nie prowadzi działalności w UE. WP29 wnosi o to, by w projekcie decyzji w sprawie odpowiedniej ochrony danych osobowych informacja ta została jednoznacznie podana.

Musi istnieć jasność co do tego, że zasady Tarczy Prywatności obowiązywać będą od momentu, w którym nastąpi przekazanie danych. Dodatkowo WP29 przypomina, że administratorzy danych prowadzący działalność w UE i przekazujący dane do podmiotu przetwarzającego w USA pozostają objęci zakresem obowiązywania unijnych przepisów o ochronie danych.

1.2.2 Brak czytelności dokumentów Tarczy Prywatności

Fakt, że zasady i gwarancje ustanawiane na mocy Tarczy Prywatności wskazane są zarówno w decyzji w sprawie odpowiedniej ochrony danych osobowych, jak i w załącznikach do niej, sprawia, że informacje te trudno jest odnaleźć oraz że czasem są one niespójne. Przyczynia się to do ogólnego braku jasności nowych ram, a także utrudnia dostęp do nich osobom, których dane dotyczą, podmiotom, a także organom ochrony danych. Zostały one również sformułowane w niejasnym dla odbiorcy języku. WP29 w związku z tym wzywa Komisję, aby zagwarantowała ona, że informacje te są jasne i zrozumiałe po obu stronach Atlantyku.

WP29 sugeruje włączenie osobnego załącznika, w którym zdefiniowane zostałyby najważniejsze terminy stosowane w dokumentach Tarczy Prywatności. Wspólne i jednoznaczne zrozumienie zobowiązań nałożonych na podstawie decyzji w sprawie odpowiedniej ochrony danych osobowych Tarczy Prywatności ma kluczowe znaczenie dla jej skutecznego stosowania po obu stronach Atlantyku, w związku z czym WP29 obawia się, że ze względu na liczne odesłania do innych dokumentów, a także niespójne sformułowania i kompleksowość dokumentów ramowych, wystąpią trudności dotyczące spójności, zrozumiałości i czytelności w kontekście wdrożenia Tarczy Prywatności.

Co bardziej istotne, w dokumentach Tarczy Prywatności zastosowano terminologię, która nie jest spójna z terminologią ogólnie stosowaną w UE w odniesieniu do ochrony danych. Niekoniecznie jest to problem, o ile wiadomo, jak brzmi odpowiadający danemu wyrażeniu termin na podstawie przepisów UE (i USA). WP29 z żalem zauważa jednak, że sytuacja ta

nie ma miejsca w omawianym przypadku, co dotyczy także projektu decyzji w sprawie odpowiedniej ochrony danych osobowych. Na przykład w rozdziale 3 projektu decyzji w sprawie odpowiedniej ochrony danych osobowych termin „dostęp" użyty został w znaczeniu implikującym zbieranie danych osobowych, a nie umożliwienie innej osobie wgląd do wcześniej zebranych danych. Dostęp przedsiębiorstw do danych oraz prawo osób fizycznych do uzyskania dostępu stanowią dwie odrębne koncepcje, których nie należy mylić.

WP29 podkreśla, że w omawianych dokumentach terminologia powinna być stosowana w sposób spójny, co dotyczy również projektu decyzji w sprawie odpowiedniej ochrony danych osobowych. W obecnej sytuacji tak się nie dzieje - dotyczy to np. terminów „przetwarzanie" oraz „dane osobowe". Co do zasady oba są odpowiednio zdefiniowane w załączniku II, jednak nie są konsekwentnie stosowane w dokumentach, co prowadzi do luk w ochronie[10].'[11]

WP29 z zadowoleniem przyjmuje fakt, że definicje niektórych z użytych terminów zostały ujęte w dokumentach tworzących Tarczę Prywatności. Nie dzieje się tak jednak w przypadku szeregu innych kluczowych terminów, w tym „przedstawiciela" lub „podmiotu przetwarzającego dane", „danych kodowanych za pomocą klucza", „danych zanonimizowanych" oraz „osoby fizycznej z UE", co w opinii WP29 stanowi podstawowy warunek jednoznacznego zdefiniowana przedmiotu uzgodnień między USA a UE i pozwoli uniknąć chaosu na późniejszym etapie zarówno dla administratorów, jak i przetwarzających dane na podstawie Tarczy Prywatności, organów nadzoru jak i opinii publicznej. Prostym rozwiązaniem byłoby tu załączenie glosariusza terminów do odpowiedzi na najczęściej zadawane pytania w sprawie Tarczy Prywatności.

WP29 wskazuje także na uzasadnione przyczyny przetwarzania danych wrażliwych w zasadzie uzupełniającej nr 1 (załącznik II pkt III.1) w przypadkach, gdy podmiot nie musi otrzymać wyraźnej zgody (opt-in). Zasadę uzupełniającą nr 1 można rozumieć jako wyliczającą zgodne z prawem podstawy zbierania danych w UE, jako ze lista ta jest zbliżona do art. 8 Dyrektywy. WP29 chciałaby przypomnieć, że jakiekolwiek przetwarzanie (w tym

[10] W niektórych klauzulach zamiast zastosowania terminu „przetwarzanie" znajdują się wyłącznie wyliczenia określonych rodzajów czynności przetwarzania. Prowadzi to do powstania luk w ochronie. Np. zgodnie z brzmieniem załącznika II, sekcja III pkt 6 lit. f), zasady Tarczy Prywatności mają zastosowanie wyłącznie, gdy dany podmiot „przechowuje, wykorzystuje lub ujawnia" otrzymane dane (tj. nie w przypadku innych czynności objętych definicją terminu „przetwarzanie", takich jak zbieranie, zapisywanie, zmienianie, odzyskiwanie, usuwanie danych). Wymóg dotyczący bezpieczeństwa danych zostałby nałożony wyłącznie w odniesieniu do „tworzenia, utrzymywania, wykorzystywania lub rozpowszechniania" danych osobowych (załącznik II sekcja II pkt 4). Definicja danych osobowych także ogranicza się do danych „otrzymanych" i „zapisanych". Jako dodatkowy przykład niech służy zasada powiadomienia (załącznik II sekcja II pkt 1 lit. a) ppkt (iv)), która stanowi, że certyfikowany podmiot musi powiadomić osoby fizyczne o celach, w których „zbiera i wykorzystuje" dane na ich temat. W załączniku II sekcja III pkt 9 lit. a) ppkt (11) mowa jest wyłącznie o danych, które podlegają „przekazaniu" lub do których ktoś ma „dostęp". Mimo tego, że w większości przypadków wydaje się, że celem nie było ograniczenie zakresu stosowania zasad lub stworzenie luk w ochronie, ta niespójna terminologia generuje ryzyko powstania takich luk. W związku z tym, że termin „przetwarzanie" jest zdefiniowany w zasadach, kluczowe znaczenie ma wykorzystywanie go w sposób spójny w celu uniknięcia występujących obecnie luk. W innym przypadku zostałoby zbyt wiele miejsca na potencjalnie niezamierzoną interpretację, która mogłaby prowadzić do nieprawidłowej interpretacji brzmienia decyzji.

[11] Definicja „danych osobowych" zawarta w załączniku II sekcja I pkt 8 lit a), mówi o „danych dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej". W zasadzie uzupełniającej stwierdzono jednak, że w odniesieniu do danych dotyczących zasobów ludzkich zasady obowiązują jedynie wtedy, gdy „przekazywane lub udostępniane są indywidualnie zidentyfikowane zapisy". WP29 uważa, że tworzy to możliwość przetwarzania danych osobowych w sposób, który jest niezgodny z zasadami ochrony danych na podstawie przepisów UE, czy też z ogólną definicją danych osobowych na podstawie Tarczy Prywatności.

zbieranie i przekazywanie) danych wrażliwych objętych przepisami UE musi posiadać uzasadnione przyczyny zgodnie z art. 8 Dyrektywy. Tarcza Prywatności nie może oferować alternatywnych podstaw dla takiego przetwarzania. Na przykład zdaniem WP29 nie jest dopuszczalne, by podmiot amerykański zbierał dane podlegające przepisom UE na podstawie amerykańskiego prawa pracy (zob. załącznik II sekcja III pkt1 lit. a) ppkt (v)). WP29 w związku z tym podkreśla, że jakakolwiek interpretacja zasady uzupełniającej nr 1 może prowadzić wyłącznie do jej zastosowania względem danych wrażliwych już przekazanych po ich zebraniu w UE na podstawie uzasadnionych przyczyn, o których mowa w art. 8 Dyrektywy.

WP29 zwraca wreszcie uwagę, na niejasność w zakresie tego, kto może być uznany za obywatela UE i tym samym beneficjenta ochrony na podstawie Tarczy Prywatności: wszyscy obywatele UE czy wszystkie osoby zamieszkałe w UE. Ma to szczególne znaczenie w odniesieniu do prawa do środków odwoławczych, w tym dostępu do instytucji Rzecznika. Dodatkowo decyzja w sprawie odpowiedniej ochrony danych osobowych powinna uwzględniać kwestię zakresu obowiązywania postanowień Tarczy Prywatności w odniesieniu do obywateli/mieszkańców państw EOG i Szwajcarii, którzy w przeszłości objęci byli programem „bezpieczna przystań".

1.2.3 Wspólny przegląd i zawieszenie

WP29 z zadowoleniem przyjmuje fakt, że Komisja Europejska i władze USA uzgodniły regularny przegląd stosowania Tarczy Prywatności w praktyce. Taki wspólny przegląd jest od szeregu lat znaną praktyką wśród społeczności ochrony danych w UE, szczególnie w odniesieniu do porozumień w sprawie wymiany danych PNR z państwami trzecimi i porozumienia TFTP. WP29 dodatkowo z zadowoleniem przyjmuje fakt, że we wspólnych przeglądach może brać udział nieokreślona liczba przedstawicieli organów ochrony danych.

Biorąc pod uwagę swoje doświadczenia w prowadzeniu w ostatnich latach wspólnych przeglądów WP29 chciałaby zdecydowanie stwierdzić, że oczekuje, iż wspólny przegląd Tarczy Prywatności będzie bardziej kompleksowy niż wspólne przeglądy PNR i TFTP. W szczególności należy zadbać o to, by wspólne przeglądy obejmowały nie tylko spotkania z przedstawicielami amerykańskich urzędów, podmiotów i przedsiębiorstw, lecz także kontrole na miejscu stosowania pewnych elementów Tarczy Prywatności. Przedstawiciele organów ochrony danych (DPA) w ramach wspólnego przeglądu powinni móc przekazywać sugestie w sprawie takich kontroli na miejscu.

WP29 uważa, że wspólny przegląd wymaga wspólnej oceny ustaleń. Do tej pory wyniki wspólnych przeglądów były prezentowane w dokumencie roboczym Komisji, który nie musiał być zatwierdzony przez członków zespołu ds. wspólnego przeglądu spoza Komisji. W przypadku wspólnego przeglądu Tarczy Prywatności WP29 byłaby wdzięczna, gdyby raport z wnioskami mógł być naprawdę wspólnym dziełem. Jako alternatywę rozważyć można opublikowanie odrębnego sprawozdania DPA ze wspólnego przeglądu.

I wreszcie, w odniesieniu do wspólnego przeglądu, WP29 przypomina o obietnicy Komisji, że koszty poniesione przez przedstawicieli WP29 w trakcie wspólnych przeglądów podlegać będą zwrotowi przez Komisję. Grupa Robocza zakłada, że tak będzie również w przypadku wspólnego przeglądu Tarczy Prywatności, w każdym razie dla rozsądnej liczby przedstawicieli DPA.

WP29 zaleca, by przynajmniej trzy miesiące przed pierwszym wspólnym przeglądem Tarczy Prywatności Komisja, władze USA i WP29 uzgodniły między sobą i spisały jego warunki.

1.2.4 Ramy UE podlegające przeglądowi

Decyzja w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA jest pierwszą decyzją w sprawie odpowiedniej ochrony danych osobowych, która została sporządzona w następstwie zasadniczej zgody co do tekstu ogólnego rozporządzenia w sprawie ochrony danych. WP29 ustaliła jednak, że Tarcza Prywatności nie odzwierciedla jeszcze tej przyszłej sytuacji. Na przykład w Tarczy Prywatności nie znalazły się istotne nowe koncepcje, takie jak prawo przenoszenia danych i dodatkowe zobowiązania ciążące na administratorach danych, w tym konieczność prowadzenia ocen skutków w zakresie ochrony danych oraz zapewnienia zgodności z zasadami uwzględnienia ochrony prywatności już w fazie projektowania i domyślnej ochrony prywatności. WP29 w związku z tym pragnie zasugerować, by Tarcza Prywatności, podobnie jak inne obowiązujące decyzje w sprawie odpowiedniej ochrony danych osobowych, została poddana przeglądowi zaraz po wejściu w życie ogólnego rozporządzenia w sprawie ochrony danych (GDPR). Pożądanym działaniem byłoby umieszczenie wyraźnego odwołanie do wspomnianego przeglądu w ostatecznej wersji decyzji w sprawie odpowiedniej ochrony danych osobowych.

2. OCENA CZĘŚCI HANDLOWEJ PROJEKTU DECYZJI W SPRAWIE ODPOWIEDNIEJ OCHRONY DANYCH OSOBOWYCH

2.1 Uwagi ogólne

2.1.1 Ulepszenia

WP29 z zadowoleniem przyjmuje ulepszenia, które wprowadza Tarcza Prywatności, a także wolę negocjatorów, by spróbować wyeliminować wskazane przez WP29 niedociągnięcia w programie „bezpieczna przystań". W szczególności w porównaniu do programu „bezpieczna przystań" ulepszenia odnotowano w następujących elementach: wprowadzono niektóre kluczowe definicje, takie jak „dane osobowe", „przetwarzanie" i „administrator", stworzono mechanizmy w celu zapewnienia nadzoru nad wykazem podmiotów uczestniczących w programie Tarczy Prywatności i obecnie obowiązkowe zewnętrzne i wewnętrzne przeglądy pod kątem zgodności. Ulepszono także zasadę dostępu, w związku z czym WP29 odnotowuje, że w obecnej wersji przewidziano prawo do poprawiania i usuwania danych w przypadku wykorzystania danych w sposób niezgodny z zasadami Tarczy Prywatności. Dodatkowo wyraźnie wskazano, że osoba fizyczna musi otrzymać zarówno potwierdzenie, że dotyczące jej dane są przetwarzane, jak i komunikat dotyczący przetworzonych danych.

WP29 z zadowoleniem także przyjmuje wzmocnienie gwarancji prawnych w sytuacjach dalszego przekazywania, a także zobowiązania Departamentu Handlu (DoC) i Federalnej Komisji Handlu (FTC) w zakresie egzekwowania obowiązków ustanowionych w Tarczy Prywatności.

2.1.2 Zastosowanie Tarczy Prywatności wobec podmiotów działających jako przetwarzający dane (przedstawiciel)

Zakres obowiązywania zasad Tarczy Prywatności względem certyfikowanych podmiotów otrzymujących dane osobowe z UE wyłącznie w celu ich przetworzenia (zwanych „przedstawicielami" lub „podmiotami przetwarzającymi dane"), wciąż jest niestety niejasny. W postanowieniach zawartych w załączniku II sekcja III pkt 10 lit. a), wspomina się o przekazywaniu danych do certyfikowanych podmiotów w takich celach, tj. wspominając wymóg zawarcia umowy, to brakuje w jednak nich wskazania, w jaki sposób zasady Tarczy Prywatności mają zastosowanie do takich podmiotów przetwarzających dane (przedstawicieli). Jest to źródłem niepewności zarówno dla certyfikowanych amerykańskich podmiotów otrzymujących dane w celu ich przetworzenia, spółek UE przekazujących dane do certyfikowanych podmiotów działających jako przetwarzający, jak i dla osób, których dane są przetwarzane. W rezultacie trudno będzie ustalić, które obowiązki mają faktycznie zastosowanie wobec podmiotów uczestniczących w Tarczy Prywatności przetwarzających dane osobowe otrzymane z UE działających w charakterze przetwarzających. Z pewnością konieczne jest wyjaśnienie tej kwestii.

Ze względu na fakt, że to zawsze administrator danych (zob. definicja „administratora" w załączniku II sekcja I pkt 8 lit. c)) ustala cel i środki przetwarzania danych, należy wziąć pod uwagę, że szereg zobowiązań ujętych w zasadach nie ma zastosowania do przetwarzających. Z tego względu niektóre zobowiązania zawarte w zasadach, gdyby zastosować je względem podmiotu działającego w charakterze przedstawiciela, mogą być sprzeczne z umową o przetwarzanie danych wymaganą przez prawo UE (umową, o której mowa w załączniku II, sekcja III pkt 10 lit. a)). Umowa o przetwarzanie danych zasadniczo nie zezwoli na przykład przetwarzającemu (przedstawicielowi) na dalsze przekazywanie danych do administratora będącego osobą trzecią, nawet w okolicznościach wskazanych w załączniku II, sekcja II pkt 3 lit. a). Dalsze przekazywanie do przedstawicieli będących osobami trzecimi powinno być dopuszczone wyłącznie za wcześniejszą zgodą administratora danych. Dodatkowo zgodnie z wymaganiami prawa UE przetwarzający (przedstawiciel) nie będzie mógł przekazać osobom pełnego powiadomienia zgodnie z intencją zasady powiadamiania (załącznik I sekcja II pkt 1), na przykład dlatego, że ten podmiot nie ustala celów przetwarzania.

W związku z tym kluczowe jest wyjaśnienie w zasadach, że w przypadku takiej sprzeczności obowiązują postanowienia umowy o przetwarzanie danych, a w szczególności instrukcje podmiotu przekazującego dane poza UE. Bez takiego wyjaśnienia zasady mogłyby być interpretowane i stosowane w sposób, który oferuje zbyt wiele możliwości kontroli przedstawicielowi podmiotu Tarczy, co z kolei narażałoby podmiot przekazujący dane z UE na ryzyko naruszenia jego zobowiązań jako administratora danych na podstawie przepisów ochrony danych UE, którym podlega przekazując dane do podmiotu Tarczy działającego w

charakterze przedstawiciela. Dodatkowo ta niejasność pozwala przypuszczać, że przetwarzający mógłby ponownie wykorzystywać te dane w dowolnie wybrany przez siebie sposób.

Należy także ustanowić szczegółowe zasady dotyczące sytuacji, w których podmiot działa jako przetwarzający (przedstawiciel) po to by zagwarantować, że postępuje on zgodnie z instrukcjami administratora danych. Należy wyraźnie wskazać, że amerykańskie podmioty otrzymujące dane wyłącznie w celu przetwarzania nie mogą decydować o przetwarzaniu tych danych we własnym imieniu. W sytuacji braku konkretnych zasad obowiązujących względem podmiotów działających jako przetwarzający ciężko jest ustalić na podstawie jakich zasad przetwarzający (przedstawiciel) miałby możliwość samodzielnej certyfikacji.

2.1.3 Ograniczenia obowiązku przestrzegania zasad

W załączniku II sekcja I pkt 5 przewidziano między innymi wyłączenia z obowiązku przestrzegania zasad w przypadku, gdy dane objęte Tarczą Prywatności wykorzystywane są z powodu kwestii związanych z bezpieczeństwem narodowym[12], interesem publicznym, egzekwowaniem prawa lub na podstawie ustaw, rozporządzeń lub orzecznictwa, które tworzy sprzeczne zobowiązania lub jednoznaczne upoważnienia. Bez pełnej wiedzy o prawie USA na poziomie federalnym i stanowym ciężko jest grupie WP29 ocenić zakres tego wyłączenia i stwierdzić, czy ograniczenia te są uzasadnione w społeczeństwie demokratycznym. Niezwykle istotne byłoby uwzględnienie przez Komisję Europejską w projekcie decyzji w sprawie odpowiedniej ochrony danych osobowych analizy stopnia ochrony w przypadku, gdyby wyłączenia takie miały obowiązywać. WP29 wzywa Komisję do zagwarantowania, że UE posiada wiedzę o ustawach lub rozporządzeniach władz, które wpływałyby na te zasady, co dotyczy zarówno ustaw jak i rozporządzeń obowiązujących teraz i w momencie ich wejścia w życie.

2.1.4 Brak zasady ograniczenia przechowywania danych

Zasada ograniczania przechowywania danych (art. 6 ust. 1 lit. e) Dyrektywy) stanowi fundamentalną zasadę prawa ochrony danych UE wymagającą, by dane osobowe przechowywane były wyłącznie przez okres konieczny do osiągnięcia celu, w którym zostały zebrane, lub w którym są dalej przetwarzane.

WP29 nie może jednak znaleźć w dokumentach tworzących Tarczę Prywatności żadnej wzmianki dotyczącej konieczności zapewnienia przez administratorów danych, by dane były usuwane po tym, jak przestanie obowiązywać cel, w którym zostały zebrane lub w którym były dalej przetwarzane. W związku z tym wydaje się, że zasady nie nakładają na certyfikowane podmioty ograniczeń co do okresu przechowywania danych porównywalnego do okresu wymagalnego na postawie prawa UE zgodnie z zasadą ograniczania przechowywania danych.

[12] Dodatkowe uwagi dotyczące wykorzystywania danych osobowych objętych Tarczą Prywatności na potrzeby bezpieczeństwa narodowego znajdują się w rozdziale 3, a na potrzeby egzekwowania prawa w rozdziale 4.

Brzmienie zasad celowości i integralności danych (załącznik II sekcja II pkt 5) w żaden sposób nie może zostać uznane za ustanawiające zobowiązanie wobec podmiotu działającego jako administrator, by usuwał on dane, gdy nie są już potrzebne do celów, w jakich były zbierane lub dalej przetwarzane, lub wobec podmiotu działającego jako przetwarzający, by usuwał on dane po rozwiązaniu umowy o świadczenie usługi.

Grupa Robocza pragnie podkreślić, że brak postanowień narzucających ograniczenia w odniesieniu do okresu przechowywania danych na podstawie Tarczy Prywatności daje umożliwia podmiotom przechowywanie danych przez dowolny okres, nawet po rezygnacji z udziału Tarczy Prywatności, co jest niezgodne z kluczowymi założeniami zasady ograniczenia przechowywania danych.

2.1.5 Brak gwarancji dla decyzji zautomatyzowanych tworzących skutki prawne lub mających istotny wpływ na osoby fizyczne

Tarcza Prywatności nie dostarcza żadnych gwarancji prawnych w sytuacji, gdy wobec danej osoby fizycznej ma zastosowanie decyzja tworząca dla niej skutki prawne lub mająca na nią istotny wpływ i która oparta jest wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych aspektów o charakterze osobistym, jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność, sposób zachowania itp.

WP29 podkreśliła już w Dokumencie Roboczym nr 12 konieczność zapewnienia gwarancji prawnych w przypadku decyzji zautomatyzowanych (tworzących skutki prawne lub mających istotny wpływ na osoby) w celu zapewnienia odpowiedniego stopnia ochrony.

Konieczność ta staje się jeszcze bardziej istotna ponieważ rozwój nowych technologii umożliwia większej liczbie przedsiębiorstw rozważenie wdrożenia zautomatyzowanych systemów decyzyjnych, co może osłabiać pozycję osób, które nie będą mogły odwołać się od decyzji podjętych przez maszynę. W sytuacji, gdy decyzje podejmowane wyłącznie przez zautomatyzowane systemy mają wpływ na sytuację prawną osób lub mają inny znaczący wpływ na takie osoby (np. poprzez dodanie do czarnej listy i tym samym pozbawienie osoby jej praw) niezwykle ważne jest zapewnienie wystarczających zabezpieczeń, w tym prawa do informacji o logice podejmowania takich decyzji i złożenia wniosku o ponowną analizę decyzji w sposób nieautomatyczny.

2.1.6 Okres przejściowy w odniesieniu do istniejących stosunków handlowych

W Tarczy Prywatności przewidziano, że jej zasady mają zastosowanie od momentu certyfikacji. Podmioty, które uzyskają certyfikację w ciągu pierwszych dwóch miesięcy od dnia rzeczywistego wejścia w życie ram Tarczy Prywatności, będą musiały zagwarantować, tak szybko jak to możliwe, że ich stosunki handlowe z osobami trzecimi spełniają warunki zasady odpowiedzialności za wtórne przekazywanie. Stan taki muszą one osiągnąć nie później niż dziewięć miesięcy od daty uzyskania certyfikacji w ramach Tarczy Prywatności.

Oznacza to, że istniejące umowy muszą zostać dostosowane do zasad w okresie od dwóch do dziewięciu miesięcy po uzyskaniu certyfikacji. Podczas tego okresu przejściowego wystarcza

stosowanie zasad powiadamiania i wyboru. WP29 zdecydowanie zaleca, by przekazywanie danych na podstawie Tarczy Prywatności mogło następować wyłącznie od momentu, w którym podmiot będzie w stanie osiągnąć zgodność ze wszystkimi wymaganiami Tarczy. Możliwość przesyłania danych w trakcie okresu przejściowego w sytuacji, gdy ich odbiorca nie może osiągnąć pełnej zgodności z zasadami Tarczy, nie może być uznana za spełnienie warunków przekazywania zgodnie z prawem i w związku z tym nie może zostać zaakceptowana.

2.2 Uwagi szczegółowe

2.2.1. Przejrzystość

a) Ogólne uwagi dotyczące zasady powiadamiania

WP29 z zadowoleniem przyjmuje bardziej kompleksowe i szczegółowe wymogi ustanowione w ramach zasady powiadamiania, a w szczególności fakt, że powiadomienie będzie musiało zawierać, łącze lub adres strony internetowej z wykazem podmiotów Tarczy Prywatności, a także wzmiankę o prawie dostępu do danych dla osób fizycznych, a także o alternatywnych mechanizmach rozwiązywania sporów[13]. WP29 sugeruje jednak, by pozostałe prawa wynikające z Tarczy wskazać w bardziej jednoznaczny sposób (prawo do poprawiania, usuwania w przypadku niepoprawności danych lub ich przetwarzania z naruszeniem zasad).

Dokumenty składające się na Tarczę Prywatności budzą wątpliwości co do terminu, w którym podmiot Tarczy Prywatności musi przekazać danej osobie powiadomienie. Załącznik II sekcja II pkt 1 lit. b) wskazuje, że „powiadomienie to musi być przekazane (...) z chwilą, gdy osoby fizyczne zostały po raz pierwszy poproszone o przekazanie danych osobowych podmiotowi lub w najbliższym możliwym terminie po zwróceniu się do tych osób o dane osobowe po raz pierwszy, ale w każdym przypadku przed użyciem przez podmiot takich danych w celu innym niż ten, w którym były one pierwotnie gromadzone lub przetwarzane przez podmiot przekazujący, lub też zanim podmiot ujawni je po raz pierwszy osobie trzeciej". WP29 uważa, że w wielu przypadkach amerykańskie podmioty Tarczy nie będą bezpośrednio zbierać danych od podmiotu, więc termin przekazania powiadomienia powinien przypadać na moment, gdy dane są rejestrowane przez podmiot Tarczy.

WP29 zwraca uwagę na fakt, że rzeczywiste wdrożenie wymagań dotyczących zasady powiadamiania oraz polityki prywatności należy ocenić podczas pierwszego rocznego przeglądu Tarczy Prywatności.

b) Podanie polityki prywatności do publicznej wiadomości

WP29 z zadowoleniem przyjmuje fakt, że wyraźnie stwierdzono, iż DoC będzie sprawdzać, czy spółki posiadające serwisy internetowe w domenie publicznej opublikowały w nich swoje

[13] Załącznik II sekcja II pkt1; WP29 odwołuje się także do drugiego zalecenia Komisji w komunikacie COM(2103) 847 a także pisma grupy WP29 z dnia 10 kwietnia 2014 r. do wiceprzewodniczącej Reding, w szczególności jego pkt 4 pod nagłówkiem „Przejrzystość".

polityki prywatności, a w sytuacji gdy nie mają takich serwisów, gdzie taka polityka prywatności podawana jest do wiadomości publicznej.[14]

c) Publikacja warunków prywatności umów z przetwarzającymi

Jako jeden z warunków, pod którymi podmioty Tarczy Prywatności mogą przekazywać dane przetwarzającym (przedstawicielom), w Tarczy Prywatności przewidziano obowiązek podmiotów, które samodzielnie przeszły certyfikację dotyczący „przekazania streszczenia lub poświadczonej kopii odpowiednich postanowień dotyczących prywatności zawartych w umowie z tym przedstawicielem" (zob. załącznik II sekcja II pkt 3 lit. b) ppkt (v)). Grupa Robocza z zadowoleniem przyjmuje wprowadzenie tego wymogu w zakresie przejrzystości wobec Departamentu Handlu.

2.2.2. Wybór

Tarcza Prywatności przewiduje prawo odmowy (klauzula opt-out) ujawnienia danych osobowych stronom trzecim lub wykorzystania danych osobowych w znacząco innym celu[15] (załącznik II sekcja III pkt 2). Dodatkowo osoby fizyczne korzystają także w dowolnym czasie z prawa odmowy wykorzystywania danych osobowych na potrzeby marketingu bezpośredniego (załącznik II sekcja III pkt 12 lit. a))[16].

Z wyjątkiem marketingu bezpośredniego nie zamieszczono szczegółów na temat sposobu i momentu realizacji takiej odmowy (zastosowania klauzuli opt-out). WP29 uważa, że zwykłe odwołanie do istnienia tego prawa w polityce prywatności nie wystarczy, natomiast należy zagwarantować, że *zindywidualizowaną* możliwość wykonywania tego prawa oferowana jest *przed* ujawnieniem lub ponownym wykorzystaniem danych osobowych.

Dodatkowo WP29 podkreśla, że w ramach Tarczy Prywatności oferowane powinno być ogólne prawo do sprzeciwu (z uzasadnionych przyczyn związanych z określoną sytuacją podmiotu danych), rozumiane jako prawo do złożenia wniosku o zakończenie przetwarzania danych takiej osoby za każdym razem, gdy ma ona zgodne z prawem i uzasadnione powody, by tak postąpić.[17]. WP29 zdecydowanie zaleca, by projekt decyzji w sprawie odpowiedniej ochrony danych osobowych jednoznacznie wskazywał, że prawo do sprzeciwu powinno mieć zastosowanie w każdym momencie, oraz że sprzeciw ten nie jest ograniczony do wykorzystywania danych na potrzeby marketingu bezpośredniego[18].

WP29 wyraża obawy, że brak definicji, „znacząco różnego" celu spowoduje chaos i niepewność prawa. Należałoby także wyjaśnić, że w każdym przypadku zasady wyboru nie

[14] Zob. pierwsze zalecenie Komisji Europejskiej w komunikacie COM(2013) 847 a także pismo grupy WP29 z dnia 10 kwietnia 2014 r do wiceprzewodniczącej Reding, w szczególności jego pkt 3 pod nagłówkiem „Przejrzystość".
[15] Zasada uzupełniająca 14c.I przewiduje prawo do wycofania się z prób klinicznych, co może być postrzegane jako prawo do sprzeciwu lub do cofnięcia zgody.
[16] Regulacja ta jest identyczna z zastosowaną w programie „bezpieczna przystań" (najczęściej zadawane pytania, nr 12) i w tym zakresie nie wprowadzono żadnych zmian.

[18] Zob. pismo WP29 do wiceprzewodniczącej Reding, pod nagłówkiem „Wybór".

można wykorzystywać do obejścia zasady celowości[19]. Zasada wyboru powinna mieć zastosowanie wyłącznie gdy cel jest znacząco różny, lecz jednak wciąż zgodny, ponieważ przetwarzanie w celu niezgodnym jest zabronione (załącznik II sekcja II pkt 5 lit. a)). Należy wyjaśnić, że prawo do zastosowania klauzuli opt-out nie może umożliwiać podmiotowi wykorzystywania danych do celów niezgodnych. W związku z tym WP29 zaleca ujednolicenie powiązanych sformułowań za pomocą zastosowania tego samego, zdefiniowanego terminu (np. „znacząco różny, lecz zgodny cel").

Przydatne byłyby zamieszczenie wyjaśnień dotyczących zastosowania prawa UE w odniesieniu do decyzji podjętych w odniesieniu do o przetwarzania danych w innym celu lub o ujawnienia informacji. W takiej sytuacji bezpośrednie zastosowanie będą miały standardowe warunki prawne UE dotyczące tego przetwarzania (takie jak zakaz przetwarzania w celach niezgodnych, konieczność przedstawienia zgodnych z prawem podstaw przetwarzania i konieczność poinformowania osoby, której dane dotyczą), także wobec podmiotów z USA podlegających prawu UE. W praktyce oznacza to, że obowiązek zapewnienia przejrzystości i zgodnego z prawem UE przetwarzania spoczywa na podmiocie przekazującym z UE podejmującym taką decyzję. W związku z tym zasada wyboru będzie miała zastosowanie wyłącznie w przypadkach gdy decyzja podejmowana jest przez podmiot amerykańską Tarczy, który nie podlega prawu UE.

2.2.3 Dalsze przekazywanie

a) Zakres

WP29 wyraża obawy w odniesieniu do sytuacji, w której następuje dalsze przekazanie danych osobowych przez podmiot z USA certyfikowany na podstawie Tarczy Prywatności do odbiorcy w państwie trzecim.

Tarczy nie należy wyłącznie postrzegać przez pryzmat przekazywania unijnych danych z UE do USA, lecz uwzględnić również kwestię przekazywania danych z USA do państw trzecich. To oznacza, że postanowienia dotyczące dalszego przekazywania stanowią istotny element Tarczy, który powinien zapewniać wystarczające gwarancje i odpowiedni poziom ochrony danych podczas ich dalszego przekazywania poza USA. Szczególną kwestią jest aspekt bezpieczeństwa narodowego i egzekwowania prawa.

Zasada odpowiedzialności za dalsze przekazywanie będąca częścią Tarczy Prywatności nie ogranicza się do odbiorców będących administratorami danych, przetwarzającymi lub przedstawicielami działającymi w USA. Dlatego dalsze przekazywanie danych do państw trzecich mogłoby odbywać się na podstawie Tarczy Prywatności, nawet jeżeli państwo trzecie posiada przepisy dotyczące dostępu organów publicznych do danych osobowych, na przykład na potrzeby inwigilacji. W odniesieniu do danych osobowych z UE stwarza to zagrożenie wystąpienia nieuzasadnionych ingerencji w zasadę ochrony praw podstawowych.

[19] Konkretny przykład dalszego niezgodnego przetwarzania, dopuszczonego na podstawie zasady wyboru przedstawiono w ramach zasady uzupełniającej w pkt 9 lit. b) ppkt (i) (zob. uwaga WP29 w tej sprawie pod punktem dotyczącym danych HR).

W każdym przypadku dalszego przekazywania danych do państwa trzeciego, każdy podmiot Tarczy Prywatności przed przekazaniem danych powinien być zobowiązany do dokonania oceny mających zastosowanie przepisów państwa trzeciego, którym podlega podmiot odbierający dane. Jeśli w wyniku tej oceny zostanie zidentyfikowane ryzyko wystąpienia znaczących i negatywnych skutków na gwarancje, zobowiązania i poziom ochrony danych zapewniane przez Tarczę Prywatności, amerykański podmiot Tarczy Prywatności działający w charakterze przetwarzającego (przedstawiciela) niezwłocznie zawiadamia administratora danych UE przed dokonaniem dalszego przekazania danych. W takim przypadku przekazujący dane ma prawo zawiesić przekazywanie danych i/lub wypowiedzieć umowę. W przypadku występowania ryzyka znacząco negatywnych skutków podmiot Tarczy działający w charakterze administratora danych nie powinien mieć uprawnień do przekazywania danych dalej, ponieważ byłoby to naruszenie jego zobowiązań dotyczących zapewnienia takiego samego stopnia ochrony w odniesieniu do dalszego przekazywania jaki wynika z zasad (zob. załącznik II sekcja II pkt 3 lit. a)).

Podobnie w przypadku zmiany obowiązującego w państwie trzecim prawa, która z dużym prawdopodobieństwem będzie mieć znacząco negatywne skutki dla gwarancji, zobowiązań i poziomu ochrony zapewnianego przez Tarczę Prywatności, amerykański podmiot uczestniczący w Tarczy Prywatności działający w charakterze przetwarzającego (przedstawiciela) powinien być zobowiązany – na mocy postanowień Tarczy Prywatności – do niezwłocznego powiadomienia przekazującego dane o takiej zmianie, nie później niż od momentu otrzymania wiadomości o takiej zmianie. W takim przypadku przekazujący dane ma prawo zawiesić przekazywanie danych lub wypowiedzieć umowę. W takim przypadku podmiot uczestniczący w Tarczy działający w charakterze administratora nie powinna mieć prawa przekazywać danych dalej, ponieważ ma on obowiązek zapewnienia takiego samego stopnia ochrony, jaki wynika z zasad (zob. załącznik II sekcja II pkt 3 lit. a)).

WP29 przypomina swoje stanowisko, że jeżeli administrator danych UE jest świadomy, że dane mogą być przekazywane są dalej do osoby trzeciej spoza USA, nawet zanim takie dane zostaną przekazane do USA, lub jeżeli administrator danych UE jest współodpowiedzialny za decyzję dopuszczającą dalsze przekazywanie danych, przekazywanie takie należy uznać za bezpośrednie przekazanie z UE do państwa trzeciego poza USA. Oznacza to, że do takich przypadków zastosowanie mają art. 25 i 26 Dyrektywy, a nie zasada dalszego przekazywania w ramach Tarczy Prywatności.

b) Przekazywanie danych przez podmiot uczestniczący w Tarczy Prywatności do administratora będącego osobą trzecią.

WP29 z zadowoleniem przyjmuje wprowadzenie obowiązku zawierania umów (załącznik II sekcja II pkt 3 lit. a) w celu zapewnienia, że administrator będący osobą trzecią zapewni co najmniej ten sam stopień ochrony co zasady Tarczy Prywatności. Celem tego jest sprawienie, by dane osobowe objęte były w dalszym ciągu odpowiednim stopniem ochrony, także po ich dalszym przekazaniu. WP29 ma jednak pewne uwagi w odniesieniu do zaproponowanych warunków.

Brak odwołania do zasady celowości

WP29 zaleca także wprowadzenie jednoznacznego odniesienia do zasady celowości (załącznik II sekcja II pkt 5) do warunków dotyczących dalszego przekazywania danych administratorowi będącemu osobą trzecią (załącznik II sekcja II pkt 3 lit. a)). Takie rozwiązanie jednoznacznie wskazywałoby, że dalsze przekazywanie nie może odbywać się w sytuacji, gdy administrator będący osobą trzecią przetwarza dane w niezgodnym celu.

Zwolnienie z konieczności zawarcia umowy w przypadku przekazywania danych między administratorami wewnątrz grupy kapitałowej

Jeżeli dane przekazywane są między administratorami wewnątrz grupy kapitałowej nie istnieje obowiązek zawarcia umowy. W takim przypadku zasady stanowią, iż ciągłość ochrony mogą zapewniać „wiążące reguły korporacyjne" (BCR) lub „inne instrumenty wewnątrzgrupowe (np. programy zgodności i kontroli)" (załącznik II sekcja III pkt 10 lit. b)). WP29 uważa, że odniesienie do „innych instrumentów wewnątrzgrupowych" nie gwarantuje wykonania prawnie wiążących zobowiązań przez innych członków grupy. Ponieważ WP29 i ustawodawstwo unijne[20] zasadniczo preferują wiążące prawnie zobowiązania w zakresie wewnątrzgrupowego przekazywania danych, konieczne jest zapewnienie, by Tarcza Prywatności nie była wykorzystywana do obchodzenia tego wymogu. WP29 przypomina, że w każdym przypadku wszelkie dalsze przekazywanie danych z USA do państw trzecich, nawet gdy zostało ono zaplanowane przed samym przekazaniem danych do USA lub gdy podlega ono wspólnemu administrowaniu z udziałem administratora danych UE[21], musi być uznane za przypadek bezpośredniego przekazania z UE do państwa trzeciego poza USA. W związku z powyższym do przekazywania danych w tym przypadku zastosowanie mają art. 25 i 26 Dyrektywy.

c) Przekazywanie danych przez podmiot uczestniczący w Tarczy Prywatności do administratora będącego osobą trzecią (przedstawiciela).

WP29 z zadowoleniem przyjmuje fakt, że w chwili obecnej podmioty odbierające, działające w charakterze przetwarzających (przedstawicieli) mają obowiązek zawarcia umowy o dalsze przekazywanie danych, niezależnie od ich zrzeszenia w Tarczy Prywatności lub korzystania z innego rozwiązania zapewniającego odpowiedni stopień ochrony. WP29 z zadowoleniem przyjmuje także obecność dodatkowych gwarancji obejmujących takie dalsze przekazywanie danych (załącznik II sekcja II pkt 3 lit. a) ppkt (i); sekcja II pkt 3 lit. a) ppkt (iii); sekcja II pkt 3 lit. a) ppkt (iv); sekcja II pkt 3 lit. a) ppkt (v); sekcja II pkt 7 lit. d)). Ostatni punkt (załącznik II sekcja II pkt 7 lit. d)) dotyczy obowiązku ponoszenia odpowiedzialności po ujawnieniu danych przedstawicielowi. Wydaje się jednak, że ta gwarancja nie będzie mieć zastosowania w przypadku, gdy podmiot zdecydował się na współpracę z DPA (zob. załącznik II sekcja III pkt 5 lit. a) i dalsze). WP29 nie rozumie powodu wprowadzenia takiego

[20] Konieczność wprowadzenia wiążących i egzekwowalnych zobowiązań podkreśla także tekst ogólnego rozporządzenia o ochronie danych, niezależnie od zastosowanych narzędzi (BCR, klauzule umowne, kodeksy postępowania lub certyfikacja).
[21] Na przykład dla danych HR.

wyłączenia i uważa, że odpowiedzialność w tym względzie powinna obowiązywać także w tym przypadku.

Brak odwołania do zasady celowości

WP29 zwraca uwagę, że zasada odpowiedzialności za dalsze przekazywanie (załącznik II sekcja II pkt 3) stanowi, że dane osobowe mogą być przekazywane osobie trzeciej działającej w charakterze przedstawiciela wyłącznie w ograniczonym i oznaczonym celu, ale nie stwierdza wprost, że te ograniczone i oznaczone cele muszą być zgodne z pierwotnym celem, do którego dane zostały zebrane, ani z instrukcjami administratora. W tym punkcie potrzebna jest większa klarowność. WP29 w związku z tym sugeruje, by zapewnić, że w decyzji w sprawie odpowiedniej ochrony danych osobowych zostaną ujęte niezbędne szczegóły, na przykład przez wprowadzenie jednoznacznego odniesienia do zasady celowości (załącznik II sekcja II pkt 5), zgodnie z którą dane nie mogą być przetwarzane (ani ujawniane) w niezgodnych celach w ramach zasady dalszego przekazywania (w uzupełnieniu zasady stosowania klauzuli opt-out).

Konieczność ustanowienia dodatkowych zobowiązań dla podmiotów uczestniczących w Tarczy Prywatności i działających w charakterze przetwarzających (przedstawicieli) przekazujących dane do innych przetwarzających (przedstawicieli).

Brak przejrzystych zasad w sytuacji, w której podmiot uczestniczący w Tarczy Prywatności działa w charakterze przedstawiciela (np. w imieniu administratora UE) powoduje powstanie luki prawnej i może doprowadzić do braku kontroli ze strony administratora UE. Podmiot uczestniczący w Tarczy Prywatności i otrzymujący dane w charakterze przedstawiciela administratora UE musi przestrzegać instrukcji administratora UE. Powinno to zostać jednoznacznie wskazane w zasadach, aby zagwarantować, że nieprzestrzeganie tych instrukcji spowoduje nie tylko naruszenie warunków umowy (załącznik II sekcja III pkt 10 lit. a ppkt (ii)) lecz także pogwałcenie zasad Tarczy Prywatności.

Możliwość przekazywania danych przez podmiot uczestniczący w Tarczy działający w charakterze przedstawiciela do przedstawiciela będącego osobą trzecią, musi być podana do wiadomości administratora i wymaga jego wcześniejszej zgody. W związku z tym należy jednoznacznie wskazać, że o tym, czy dopuszcza się dalsze przekazywanie danych decyduje umowa zawarta między przedstawicielem a administratorem UE (o której mowa w NZP 10 - „Umowy na podstawie art. 17")[22].

Obecnie obowiązujące warunki dotyczące dalszego przekazywania danych przedstawicielowi opierają się na założeniu, że podmiot uczestniczący w Tarczy działa w charakterze administratora i tym samym może sam decydować o ewentualnej interwencji przedstawiciela będącego osobą trzecią. Możliwość taka nie powinna jednak istnieć w sytuacji, gdy podmiot uczestniczący w Tarczy działa w charakterze przedstawiciela, ponieważ w takim przypadku administrator UE zostałby pozbawiony uprawnień kontrolnych.

[22] Zob. pismo WP29 do wiceprzewodniczącej Reding z 10 kwietnia 2014 r. punkt 4 pod nagłówkiem „Dalsze przekazywanie".

Odpowiednie postanowienia dotyczące prywatności zawarte w umowie z przedstawicielem będącym osobą trzecią muszą być udostępnione administratorowi i muszą zapewniać co najmniej ten sam stopień ochrony co umowa zawarta z administratorem.

2.2.4 Integralność danych i celowość

a) Proporcjonalność

Kwestią o nieco mniejszej wadze jest problem wspomniany przez WP29 w piśmie do wiceprzewodniczącej Reding, gdzie WP29 pisze, że „przetwarzanie danych osobowych, także w ścisłej zgodności z zasadami powiadamiania i wyboru może nie być proporcjonalne w odniesieniu do praw, interesów i wolności podmiotów danych lub społeczeństwa. Zasada proporcjonalności lub zasada rozsądnego działania, musi być uwzględniana na wszystkich etapach przetwarzania i powinna mieć zastosowanie łącznie z zasadami powiadamiania i wyboru”[23].

W ramach Tarczy Prywatności (załącznik II sekcja II pkt 5 lit. a)) stwierdza się, że informacje muszą być ograniczone do tego, czego dotyczy przetwarzanie. WP29 wolałaby zmianę tego sformułowania w ostatecznej decyzji w sprawie odpowiedniej ochrony danych osobowych, ponieważ sam fakt, że dane muszą być odpowiednie do celów przetwarzania nie sprawia, że przetwarzanie jest proporcjonalne. W celu zachowania zgodności z zasadą proporcjonalności przetwarzanie powinno być ograniczone do danych, które są niezbędne do danej czynności przetwarzania.

b) Dokładność

Zasada integralności danych i ograniczenia celu (załącznik II sekcja II pkt 5) stanowi również, że: „W zakresie niezbędnym do osiągnięcia tych celów podmiot musi podjąć zasadne działania w celu zapewnienia, aby dane osobowe były zgodne ze swoim przeznaczeniem, dokładne, kompletne i aktualne”. WP29 zwraca uwagę na fakt, że jest to brzmienie identyczne z brzmieniem porozumienia „bezpieczna przystań”. WP29 ma wątpliwości, czy należałoby dodać sformułowanie „w zakresie niezbędnym do tych celów” ponieważ według Grupy dokładność danych nie powinna zależeć od celu ich przetwarzania. WP29 preferowałaby sytuację, w której powiązanie to zostałoby usunięte z ostatecznej wersji decyzji w sprawie odpowiedniej ochrony danych osobowych.

c) Celowość

W przypadku przekazywania danych osobowych przez administratora danych prowadzącego działalność w UE amerykańskiemu podmiotowi, przekazujący dane powinien jednoznacznie poinformować ten amerykański podmiot o celach, w jakich pierwotnie zebrano te dane. Ma to kluczowe znaczenie dla ustalenia, czy po ich przekazaniu nastąpi zmiana celu przetwarzania, tym samym powodując konieczność zastosowania zasad powiadomienia i wyboru, oraz przyczyniłoby się do odpowiedniego podziału ryzyka i odpowiedzialności.

[23] Zob. pismo WP29 do wiceprzewodniczącej Reding z 10 kwietnia 2014 r., s. 8.

Zasada integralności danych i celowości (załącznik II sekcja II pkt 5) stanowi, że podmiot nie może przetwarzać danych osobowych w sposób niezgodny z celami, w których zostały one zebrane, lub na które zgodę wyraziła później dana osoba. Zasada wyboru (załącznik II sekcja II pkt 2) uwzględnia jednak możliwość zastosowania klauzuli zgody (opt-in) na „korzystanie" z informacji wrażliwych (tj. danych osobowych o stanie zdrowia lub leczeniu, pochodzeniu rasowym lub etnicznym, poglądach politycznych, wyznaniu i przekonaniach filozoficznych, przynależności do związków zawodowych lub informacji o życiu seksualnym danej osoby, a także danych z rejestrów karnych) w celach, które znacząco różnią się od celów w których dane były pierwotnie zbierane, lub na które zgodę wyraziła później dana osoba. Taka zgoda nie jest wymagana w sytuacjach, o których mowa w zasadzie uzupełniającej w pkt 1 lit. a) (załącznik II sekcja III pkt 1 lit. a)). W zakresie danych osobowych innych niż wrażliwe przewidziano możliwość wystąpienia (opt-out).

WP29 zwraca uwagę na fakt, że zakres zasady celowości jest różny w odniesieniu do zasady powiadomienia, wyboru oraz integralności danych i ich celowości. W istocie w tym samym tekście stosowane są terminy „niezgodny cel" i „znacząco niezgodny cel" bez wyjaśnienia ich dokładnych znaczeń[24].

WP29 wyraża swoje poważne zaniepokojenie faktem, że taka niespójność może prowadzić do wielkich trudności z pogodzeniem zasady integralności danych i celowości (załącznik II II.5) z zasadą wyboru (załącznik II sekcja II pkt 2), ponieważ jedna z nich mówi, że danych nie można przetwarzać w sposób niezgodny z celami, w których były one zebrane, natomiast druga przewiduje mechanizm wystąpienia (opt-out) w przypadku przetwarzania danych w celu znacząco innym od pierwotnego.

Tym samym zasadę wyboru można odczytywać w ten sposób, że dopuszcza ona dalsze niezgodne przetwarzanie[25]. WP29 uważa, że należy wyraźnie wskazać, że podmiot nie ma prawa przetwarzać danych w celu znacząco różnym, jeżeli ten cel jest niezgodny na podstawie zasady celowości. Innymi słowy należałoby wyraźnie wskazać, że zasada wyboru nie stanowi przesłanki dla wyłączenia obowiązywania zasady celowości.

W każdym przypadku jeżeli dalsze przetwarzanie ma być uznane za zgodne, muszą mieć zastosowanie zasady powiadomienia i wyboru.

2.2.5 Wyjątki dziennikarskie

Wyjątki dziennikarskie względem przetwarzania danych osobowych objęte są zasadą uzupełniającą 2 (załącznik II sekcja III pkt 2). Zakłada się, że postanowienia te odzwierciedlają amerykańską konstytucyjną ochronę wolności słowa. Tym samym dokumenty składające się na Tarczę Prywatności stanowią, że „dane osobowe znajdujące się

[24] WP29 stwierdziła, że stosowane są także inne wyrażenia: „wykorzystanie niezgodne z" (załącznik II sekcja III pkt 14 lit. b) ppkt (ii)), „wykorzystanie w innych celach" (załącznik II sekcja III pkt 9B, lit. i)), „wykorzystanie w celu innym niż ten, w którym były pierwotnie zebrane" (załącznik II sekcja II pkt 1 lit. b). Ta niejasność może powodować brak wystarczających gwarancji dotyczących zasady ograniczenia celu.

[25] Zob. także uwaga w sprawie zasady wyboru. WP29 uważa, że fakt, że zasady dalszego przekazywania (załącznik II sekcja II pkt 3) mówią jedynie o zasadzie wyboru, a nie o zasadzie celowości, zwiększa ryzyko takiej właśnie interpretacji.

w uprzednio opublikowanym materiale rozpowszechnionym z archiwów środków masowego przekazu, nie podlegają wymaganiom zasad Tarczy Prywatności" (załącznik II sekcja III pkt 2 lit. b)). Wyłączenie to zdaje się obejmować także dalsze przetwarzanie przez dowolnego administratora lub przetwarzającego, nie tylko dalsze przetwarzanie w celach dziennikarskich. Jak wspomniano w piśmie do wiceprzewodniczącej Reding z dnia 10 kwietnia 2014 r. WP29 preferowałaby większe ograniczenie stosowania wyjątków dziennikarskich, bliższe zasadzie stosowanej w UE, a także prawo do usunięcia z wykazów (prawo do bycia zapomnianym) w następstwie sprawy Google Hiszpania[26].

2.2.5 Prawo osób, których dane dotyczą do dostępu, poprawienia i usunięcia danych

Zgodnie z Tarczą Prywatności osoby mają prawo uzyskać *potwierdzenie,* czy ich dane są przetwarzane przez podmiot, a także *uzyskać informacje* o takich danych (załącznik II sekcja III pkt 8 lit. a) ppkt (i)). Zobowiązanie podmiotu do odpowiedzi na zapytania tych osób dotyczące celów przetwarzania, kategorii danych osobowych, które podlegają przetwarzaniu lub odbiorców lub kategorii odbiorców, którym ujawniane są dane osobowe nie zostało wyraźnie ujęte. WP29 uważa, że szczegółowe informacje, które należy przekazać osobie, której dane dotyczą, powinny być wskazane w tekście, a nie tylko w przypisie i powinny być ujęte w formie jednoznacznego zobowiązania (powiązanego z załącznikiem II sekcja III pkt 8 lit. a) ppkt (i)1).

Zgodnie z zasadą uzupełniającą 8 „dostęp musi zostać udzielony wyłącznie w zakresie, w jakim dany podmiot przechowuje dane osobowe" (załącznik II sekcja III pkt 8 lit. d) ppkt (ii)). Ta zasada nie powinna mieć interpretacji zawężającej w tym sensie, że należy zapewnić co do zasady dostęp do danych w jakikolwiek sposób przetwarzanych przez podmiot, a nie tylko do tych, które podmiot przechowuje. Dlatego w celu zwiększenia skuteczności prawa do dostępu istotne jest jednoznaczne wskazanie, że „przechowuje" oznacza „przetwarza" w rozumieniu definicji podanej w załączniku II sekcja I pkt 8 lit. b). Zastosowanie tej zasady należy uważnie przeanalizować podczas wspólnego przeglądu Tarczy Prywatności.

Pozostają również wątpliwości co do listy wyjątków podanej w załączniku II sekcja III pkt 8 lit. e) ppkt (i), która jest zbliżona do listy z NZP 8 programu „bezpieczna przystań", i która zdaje się przechylać szalę w stronę interesów podmiotów. W tym sensie dostęp do własnych danych osobowych nie będzie udzielany osobom z następujących przyczyn: „naruszenie poufności wymiany informacji między prawnikiem a klientem lub innej tajemnicy zawodowej lub obowiązku zawodowego" (załącznik II sekcja III pkt 8 lit. e) ppkt (3), „niekorzystny wpływ na przebieg postępowań sprawdzających pracowników lub postępowań dotyczących skarg wniesionych przez pracowników lub niekorzystny wpływ na przebieg procedur związanych z planowaniem zmian kadrowych lub reorganizacją przedsiębiorstwa" (załącznik II sekcja III pkt 8 lit. e) ppkt (4) oraz „naruszenie poufności niezbędnej do pełnienia funkcji kontrolnych, nadzorczych lub regulacyjnych związanych z prawidłowym zarządzaniem lub poufności w ramach przyszłych lub obecnie prowadzonych negocjacji z udziałem podmiotu "

[26] Sprawa C-131/12 – Google Hiszpania przeciwko Agencia Española de Protección de Datos and Mario Costeja González, 13 maja 2014 r.

(załącznik II sekcja III pkt 8 lit. e) ppkt (5). Przyczyny te należy interpretować jako uzupełniające w odniesieniu do ogólnego wyłączenia dotyczącego poufnych informacji handlowych, o którym mowa w załączniku II sekcja III pkt 8 lit. c). W związku z powyższym osoba, której dane dotyczą nie uzyska nigdy dostępu do własnych danych w sytuacjach wskazanych powyżej, zatem nie osiągnięto równowagi między prawami a interesami osób a prawami i interesami podmiotów i tym samym nie znaleziono rozwiązania kwestii dotyczącej wniosków o udostępnienie danych.

WP29 przypomina, że prawo do dostępu do własnych danych przyznawane jest osobom fizycznym na mocy art. 8 ust. 2 Karty. Chociaż nie jest to bezwzględnie obowiązujące prawo, stanowi ono fundament prawa do ochrony danych osobowych, ponieważ ułatwia egzekwowanie innych praw osób, których dane dotyczą danych, takich jak prawo do poprawienia lub usunięcia.

Jeżeli chodzi o prawo do poprawienia i usunięcia danych WP29 z zadowoleniem przyjmuje znaczną poprawę zasad Tarczy Prywatności w porównaniu z zasadami programu „bezpieczna przystań" związaną z tym, że prawa te udzielane są nie tylko w sytuacjach, w których dane są niedokładne, lecz także gdy dane zostały przetworzone z naruszeniem zasad (załącznik II sekcja II pkt 6).

2.2.6 Ochrona prawna, egzekwowanie prawa i odpowiedzialność (mechanizmy ochrony prawnej)

a) Skuteczne wykonywanie praw do środków odwoławczych osób fizycznych z UE.

WP29 przyjmuje do wiadomości zobowiązania władz amerykańskich w zakresie różnych poziomów mechanizmu środków odwoławczych. Biorąc jednak pod uwagę złożoność i niejasność ogólnej budowy tego mechanizmu WP 29 obawia się, że w praktyce mogą wystąpić przeszkody w skutecznej realizacji tego prawa przez osobę, której dane dotyczą. WP 29 wskazuje, że jakość mechanizmu środków odwoławczych powinna być istotniejsza niż ilość mechanizmów dostępnych dla osób fizycznych z UE. Istnieją również obawy, że większość, jeśli nie wszystkie mechanizmy odwoławcze, przewidują postępowanie w USA i tym samym komplikują monitorowanie tej procedury przez unijne organy ochrony danych.

W rzeczywistości mechanizm środków prawnych przewidziany w Tarczy Prywatności koncentruje się przede wszystkim na umożliwieniu podmiotowi danych „dochodzenia jego praw i złożenia powództwa w sprawie o brak zgodności z zasadami prywatności w formie bezpośredniego kontaktu z amerykańską firmą objętą samocertyfikacją"[27]. Dodatkowo podmioty muszą wyznaczyć niezależny organ rozwiązywania sporów, który bada i rozstrzyga skargi osób fizycznych. WP29 z zadowoleniem przyjmuje fakt, że koszty tego organu nie obciążą osoby fizycznej.

Skargi będzie można również składać do Federalnej Komisji Handlu (FTC), nawet jeśli nie ma ona obowiązku ich rozpatrywania. Organy ochrony danych osobowych także mogłyby

[27] Komisja Europejska, Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych, motyw 30

przesłać skargę, a Departament Handlu zobowiązał się do przeglądu i podjęcia wszelkich starań, by usprawnić rozwiązywanie sporów (załącznik I), które będą „traktowane priorytetowo" przez Federalną Komisję Handlu (załącznik II sekcja III pkt 7 lit. e)). Nadanie przez FTC priorytetu skargom nie daje jednak żadnej pewności osobie, której dane dotyczą, że jej skargi zostaną rozpatrzone.

Jako ostatni środek odwoławczy przewidziano, iż osoby fizyczne mają również prawo poddać sprawę pod arbitraż. Postępowanie arbitrażowe prowadzone będzie w USA i podlegać będzie weryfikacji sądów USA.

Tarcza Prywatności oferuje także podmiotom możliwość wyboru współpracy z unijnymi organami ochrony danych (załącznik II sekcja III pkt 5 lit. a)). Jest to nawet obowiązek w przypadku danych o zasobach ludzkich zebranych w kontekście stosunku pracy (załącznik II sekcja III pkt 9 lit. d) ppkt (ii). W takiej sytuacji nie mają zastosowania alternatywne metody rozwiązywania sporów (ADR) (załącznik II sekcja III pkt 5 lit. a)). W ramach Tarczy Prywatności nie ustalono jednoznacznie praktycznych elementów współpracy z unijnymi organami ochrony danych. W szczególności niejasne jest, czy panel arbitrażowy rozpatrywać będzie wszystkie przypadki, czy każdy przypadek będzie rozpatrywany oddzielnie przez inny panel.

WP29 uważa, że w decyzji w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności należy zapewnić większy poziom szczegółowości, jeżeli chodzi o uprawnienia organów ochrony danych do rozpatrywania skarg. Wydaje się, że zależą one od klasyfikacji podmiotu, ale nie jest jasne w jaki sposób.

W przypadku, gdy podmiot działa jako przedstawiciel w imieniu administratora UE, osoby fizyczne będą miały w każdym przypadku możliwość złożenia skargi do właściwego organu ochrony danych w UE. Podobna sytuacja będzie miała miejsce w przypadku przetwarzania danych w celach związanych z zasobami ludzkimi i przetwarzania danych do innych celów komercyjnych.

Jeżeli podmiot uczestniczący w Tarczy Prywatności działa w charakterze administratora danych, upoważnienie DPA do rozpatrywania skargi będzie ograniczone do przetwarzania objętego prawem UE (przetwarzanie na odpowiedzialność administratora UE - w tym wspólne administrowanie razem z podmiotem z USA, lub jeśli podmiot uczestniczący w Tarczy Prywatności bezpośrednio podlega prawu UE, na przykład korzystając ze sprzętu w UE. W przypadku jednak przetwarzania danych wyłącznie na podstawie przepisów USA, zastosowanie mieć będą wyłącznie mechanizmy Tarczy Prywatności. W celu przezwyciężenia bariery językowej i braku znajomości systemu prawnego USA pomocne mogłoby okazać się upoważnienie DPA z UE do działania w charakterze pośrednika w przypadku skarg składanych przez osoby fizyczne lub pomocy tej osobie w procedurach alternatywnego rozwiązywania sporów z podmiotami z USA lub w kontaktach z władzami USA, jeśli organy ochrony danych uznają to za odpowiednie.

WP29 podkreśla, że mechanizm wyjaśniony w dokumentach Tarczy Prywatności nie jest zgodny z wcześniejszym zaleceniem, zgodnie z którym osoby fizyczne z UE powinny „móc wnosić pozwy o odszkodowanie w Unii Europejskiej" a także „uzyskać prawo do złożenia pozwu przed właściwym sądem krajowym w UE".[28] Pozytywnie odebrane byłoby uwzględnienie takiej możliwości w politykach prywatności podmiotów objętych Tarczą Prywatności.

W celu zapewnienia skuteczności WP29 zaleca, by w ramach systemu umożliwić organom ochrony danych z UE reprezentowanie osoby, której dane dotyczą i działanie w jej imieniu lub w charakterze pośrednika. Ewentualnie Tarcza Prywatności powinna zawierać szczegółowe klauzule prerogacyjne, umożliwiające osobom, których dane dotyczą egzekwowanie ich praw w Europie.

b) Postępowanie arbitrażowe

Ostateczne procedury arbitrażowe nie zostały jeszcze sfinalizowane, co utrudnia przeprowadzenie analizy przez WP29. Na chwilę obecną wydaje się, że program arbitrażu będzie realizowany zgodnie z prawem USA i że jedynym językiem postępowania będzie angielski. Organy ochrony danych z UE mogą dążyć do uzyskania upoważnienia do udzielania pomocy osobom fizycznym w tym procesie.

Dodatkowo postępowanie arbitrażowe zostało wprowadzone ze względu fakt braku gwarancji, że skarga zostanie rozpatrzona, ponieważ FTC nie ma obowiązku rozpatrywania każdej skargi. WP29 zwraca uwagę, że gdyby osoba fizyczna z UE chciała uzyskać pomoc pełnomocnika, musi ona pokryć własne koszty zastępstwa procesowego, co może uniemożliwiać osobom fizycznym składanie skarg w ramach postępowania arbitrażowego.

c) Nadzór, egzekwowanie prawa i skuteczność mechanizmów odwoławczych

<u>Warunki objęcia programem Tarczy</u>

Zgodnie z TSUE „wiarygodność takiego systemu […] polega w istocie na wprowadzeniu skutecznych mechanizmów wykrywania i kontroli pozwalających na zidentyfikowanie i ukaranie w praktyce ewentualnych naruszeń reguł zapewniających ochronę praw podstawowych […]."[29]

WP29 zwraca uwagę na fakt, że rola Departamentu Handlu w zakresie Tarczy Prywatności w procesie certyfikacji wydaje się być ograniczona wyłącznie do sprawdzenia kompletności dokumentów. Chociaż WP29 przyjmuje do wiadomości, że samocertyfikacja nie zakłada systematycznej wcześniejszej kontroli wdrożenia polityk ochrony prywatności, jednak Departament Handlu powinien zobowiązać się co najmniej do systematycznej kontroli, czy polityki ochrony prywatności obejmują wszystkie zasady Tarczy Prywatności. Zobowiązanie takie jest wymienione w projekcie decyzji w sprawie odpowiedniej ochrony danych

[28] Zob. pismo WP29 do wiceprzewodniczącej Reding z 10 kwietnia 2014 r.
[29] TSUE, Schrems, pkt. 81

osobowych, ale nie można go jednoznacznie odnaleźć w piśmie z oświadczeniem Departamentu Handlu.[30]

Naruszenie zasad Tarczy Prywatności może przez długi czas pozostać niezauważone i zostać wykryte dopiero po poważnym naruszeniu praw podstawowych przysługujących osobie, której dane dotyczą, być może nawet bez możliwości naprawy zaistniałej sytuacji. Takie podejście może być sprzeczne ze europejską zasadą ostrożnościową.

Przejrzystość osiągana za pomocą wykazu podmiotów uczestniczących w Tarczy Prywatności i rejestru podmiotów usuniętych z wykazu

Jeżeli chodzi o kwestię przejrzystości w odniesieniu do osób, których dane dotyczą poczyniono znaczne postępy. Oprócz wszystkich podmiotów, które przeprowadziły samocertyfikację w Departamencie Handlu nowy wykaz Tarczy Prywatności zawierać będzie rejestr wszystkich podmiotów usuniętych z wykazu Tarczy Prywatności, w tym przyczynę usunięcia danego podmiotu[31]. Strona internetowa Tarczy Prywatności prowadzona przez Departament Handlu będzie koncentrować się bardziej na odbiorcach docelowych w ten sposób, że będzie usprawniać weryfikację rodzaju informacji objętych samocertyfikacją podmiotów, a także kontrolę polityki ochrony prywatności, która dotyczy objętych nią informacji oraz sposobu wykorzystywanego przez podmiot do sprawdzenia jej zgodności z zasadami[32]. WP29 z zadowoleniem przyjmuje fakt, że zostało obecnie jednoznacznie wskazane, że Departament Handlu będzie sprawdzać, czy spółki posiadające serwisy internetowe w domenie publicznej opublikowały w nich swoje polityki ochrony prywatności, lub w sytuacji gdy nie mają takich serwisów, gdzie taka polityka ochrony prywatności podawana jest do wiadomości publicznej.[33]. W dokumentach wspomina się również więcej o treści polityki prywatności[34].

WP29 uważa, że może pojawić się problem, gdy podmiot, która figuruje w wykazie Tarczy Prywatności rozszerzy później swój certyfikat na więcej kategorii danych. W takim przypadku wykaz nie będzie uwzględniać różnych okresów zastosowania zasad względem różnych kategorii danych. Tworzy to ryzyko, że osoby fizyczne i przedsiębiorstwa UE nie będą mogły w pełni ocenić, czy konkretny zbiór danych rzeczywiście podlega zasadom Tarczy Prywatności, a jeśli tak - od kiedy. Aby wyeliminować to niedociągnięcie, Grupa Robocza rekomenduje, by w rejestrze podmiotów w wykazie Tarczy Prywatności osobno wskazywano dla każdej kategorii danych osobowych datę wejścia w życie samocertyfikacji.

WP29 z zadowoleniem przyjmuje fakt, że Departament Handlu będzie prowadzić rejestr podmiotów, które zostały usunięte z wykazu Tarczy Prywatności, a także że rejestr ten będzie

[30] Komisja Europejska, Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych, art. 34
[31] Załącznik I, s. 5, oraz załącznik II sekcja II pkt 1; WP29 odsyła także do czwartego zalecenia Komisji w komunikacie COM(2103) 847 a także pisma grupy WP29 do wiceprzewodniczącej Reding z dnia 10 kwietnia 2014 r., w szczególności jego pkt 5 pod nagłówkiem „Przejrzystość".
[32] Załącznik I, s. 8; WP29 odsyła także do swojego pisma do wiceprzewodniczącej Reding z dnia 10 kwietnia 2014 r., w szczególności jego pkt 2 pod nagłówkiem „Przejrzystość".
[33] Załącznik I, s. 3 i 4; WP29 odnosi się także do pierwszego zalecenia Komisji w komunikacie COM(2103) 847 a także pisma WP29 do wiceprzewodniczącej Reding z dnia 10 kwietnia 2014 r., w szczególności jego pkt 3 pod nagłówkiem „Przejrzystość".
[34] Załącznik I, s. 5 i 6 oraz załącznik II sekcja III pkt 6;

zawierał wyjaśnienia, że podmioty takie nie otrzymują już gwarancji otrzymywania korzyści z tytułu przynależności do Tarczy Prywatności, lecz w dalszym ciągu muszą stosować zasady względem danych osobowych otrzymanych w czasie, kiedy były one certyfikowanymi podmiotami uczestniczącymi w programie Tarcza Prywatności, o ile przechowują one takie dane (załącznik I, s. 3). Ponieważ jednak niektóre podmioty usunięte z wykazu Tarczy Prywatności mogą podjąć decyzję o tym, by zwrócić lub usunąć dane otrzymane na podstawie Tarczy Prywatności, natomiast inne podmioty przechowywać będą dane, które otrzymały na podstawie Tarczy, ważne jest zagwarantowanie większej przejrzystości tej kwestii dla osób fizycznych. Dlatego w rejestrze spółek utrzymywanym przez Departament Handlu należy określić, czy dany podmiot w dalszym ciągu przechowuje dane osobowe otrzymane w ramach Tarczy Prywatności, czy może zwrócił lub usunął takie dane. Jeśli dany podmiot wciąż przechowuje takie dane, rejestr powinien jednoznacznie postanawiać, że podmiot w dalszym ciągu musi stosować zasady względem takich danych.

Dodatkowo rejestr prowadzony przez Departament Handlu powinien wskazywać, że podmioty te nie otrzymują już gwarancji korzyści wynikających z przynależności do programu Tarczy Prywatności na potrzeby nowych przypadków przekazywania danych, co oznacza, że podmiot nie może już otrzymywać danych osobowych z UE na podstawie zasad.

Procedury kontroli

W celu skontrolowania, czy samocertyfikacja jest w praktyce skuteczna podmioty mogą prowadzić samooceny lub zewnętrzne przeglądy zgodności. WP29 wyraża żal, że szkolenie pracowników wymagane jest wyłącznie wtedy, gdy podmiot przystępuje do weryfikacji w formie samooceny (załącznik II sekcja III pkt 7 lit. c)). Wydaje się również, że obowiązek sprawdzenia, czy polityki są właściwe, kompleksowe, umieszczone w widocznym miejscu, wprowadzone w życie i dostępne występuje tylko jeżeli podmiot przystąpi do przeglądu wewnętrznego (samooceny), a przegląd w formie mechanizmu zewnętrznego ograniczony jest do sprawdzenia zgodności polityki ochrony prywatności danego podmiotu.

A posteriori

WP29 z zadowoleniem przyjmuje fakt, że Federalnej Komisji Handlu i Departamentowi Handlu powierzono uprawnienia dochodzeniowe w zakresie skarg. Dodatkowo WP29 pragnie zauważyć, że Departament Handlu będzie mieć możliwość prowadzenia kontroli z urzędu, przede wszystkim poprzez wysyłanie kwestionariuszy. WP29 chciałaby jednak upewnić się, że takie podejście wystarczy do realizacji wymagania TSUE w zakresie skutecznych mechanizmów wykrywania naruszeń i nadzoru. WP29 wciąż ma pytania dotyczące szczegółowych uprawnień amerykańskich organów egzekwowania prawa w zakresie prowadzenia kontroli na miejscu na terenie podmiotów, które przeprowadziły samocertyfikację, w celu prowadzenia dochodzeń w sprawie naruszeń postanowień Tarczy Prywatności, w sprawie tego, w jaki sposób na terenie USA można uzyskać *exequatur* dla decyzji władz UE i w sprawie tego, czy sankcje na podstawie Tarczy Prywatności mają w praktyce funkcję odstraszającą.

2.2.7 Przetwarzanie danych o zasobach ludzkich

Zakres

Zasada uzupełniająca 9 (załącznik II sekcja III pkt 9) dotyczy danych osobowych pracownika (byłego lub obecnego) zbieranych w kontekście stosunku pracy. Zgodnie z brzmieniem zasady uzupełniającej z pkt 9 lit. a) ppkt (ii), zasady Tarczy Prywatności mają zastosowanie wyłącznie w przypadku „przekazywania indywidualnie zidentyfikowanych zbiorów danych lub uzyskiwania dostępu do takich zbiorów". Termin „zidentyfikowany zbiór danych" nie jest zgodny z definicją „danych osobowych" na podstawie załącznika II sekcja I pkt 8 lit. a), która opisuje „dane o zidentyfikowanej lub możliwej do identyfikacji osobie fizycznej" i tym samym nie jest spójna z definicją zastosowaną w Dyrektywie[35].

Zasada uzupełniająca z pkt 9 lit. a) ppkt (ii) stwierdza, że „Prowadzenie sprawozdawczości statystycznej w oparciu o zagregowane dane dotyczące zatrudnienia, które nie zawierają żadnych danych osobowych lub które nie wiążą się z wykorzystaniem zanonimizowanych danych, nie wzbudza obaw związanych z ochroną prywatności." Stanowisko to stoi w

[35] Jak już podkreślono ograniczenie do zapisów, które są „przedmiotem przekazania lub dostępu" także nie jest zgodne z terminem „przetwarzanie" (załącznik II sekcja I pkt 8 lit. b)).

sprzeczności z szeregiem opinii wydanych przez WP29. WP29 chciałaby podkreślić, że skumulowane dane mogą być również poddane ponownej identyfikacji, w związku z czym należy je traktować jak dane osobowe[36].

[36] Zob. opinia 4/2007 w sprawie koncepcji danych osobowych, a także opinia 05/2014 w sprawie technik anonimizacji.

Zasady powiadomienia, wyboru i celowości

W zasadzie uzupełniającej pkt 9 lit. b) ppkt (i) podano przykład zastosowania zasad powiadomienia i wyboru w przypadku, gdy dane o zasobach ludzkich wykorzystywane są w innym celu. Przykład ten dotyczy podmiotu z USA, który „zamierza wykorzystać dane osobowe zgromadzone w ramach stosunku pracy do celów niezwiązanych z pracą, takich jak publikacje handlowe". W tym scenariuszu zmiana celu jest dozwolona pod warunkiem zgodności z zasadami powiadamiania i wyboru. WP29 uważa, że dalsze przetwarzanie danych o zasobach ludzkich w celu prowadzenia marketingu bezpośredniego w większości przypadków trzeba będzie uznać za cel niezgodny i tym samym sprzeczny z zasadą celowości (załącznik II sekcja II pkt 5 lit. a). Dodatkowo WP29 uważa, że zasada wyboru nie może być odpowiednią podstawą dla pracownika, by wyrazić zgodę (zastosować klauzulę opt-out) na zmianę celu w kontekście zatrudnienia, gdzie taka zgoda może nie być całkowicie dobrowolna.

WP29 ma poważne wątpliwości, czy koncentracja Tarczy Prywatności na zasadzie wyboru, stanowiącej jako warunek dalszego wykorzystywania danych w innym celu, spełnia wymagania wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD) dotyczących ochrony prywatności, ponieważ brak jest wystarczających gwarancji uniemożliwiających wykorzystanie mechanizmu opt-out także do dalszego przetwarzania stanowiącego przetwarzanie niezgodne. Zasada uzupełniająca w pkt 9 lit. b) ppkt (iv) przewiduje szerokie i skonkretyzowane wyłączenie z obowiązywania zasad powiadomienia i wyboru „w okresie i w stopniu, w którym będzie to niezbędne do uniknięcia negatywnego wpływu na zdolność podmiotu do dokonywania awansów, powoływania na stanowiska lub do podejmowania podobnych decyzji dotyczących zatrudnienia". Po pierwsze już w momencie zebrania danych należy jednoznacznie wskazać wykorzystywanie danych o zasobach ludzkich w takich celach. Dodatkowo sformułowanie „podobne decyzje dotyczące zatrudnienia" jest zbyt niejasne i szerokie. Konsekwencją jego stosowania będzie to, że dane o zasobach ludzkich będą całkowicie wyłączone ze stosowania zasady powiadomienia i wyboru w ramach ich przetwarzania w kontekście stosunku pracy. Termin ten jest tak szeroki, że nie pozwala na ocenę, czy dalsze wykorzystanie jest zgodne z pierwotnym celem. WP29 zaleca usunięcie tego wyłączenia.

Prawo dostępu

Zasada uzupełniająca pkt 9 lit. e) ppkt (i) przewiduje także wyłączenie dotyczące zastosowania zasady dostępu lub konieczności zawierania umowy z administratorem będącym osobą trzecią w zakresie danych o zasobach ludzkich w sytuacji, gdy dotyczą one okazjonalnych operacji związanych z zatrudnieniem, takich jak rezerwacja lotu, pokoju hotelowego, ubezpieczenie, przekazywanie danych niewielkiej liczby pracowników z zastrzeżeniem, że zachowana będzie zgodność z zasadami powiadomienia i wyboru. WP29 nie widzi racjonalnego uzasadnienia takiego wyłączenia i zaleca skreślenie tego akapitu.

2.2.8 Produkty farmaceutyczne i wyroby medyczne

Zakres

W ramach Tarczy Prywatności uznaje się, że przekazywanie danych kodowanych za pomocą klucza z Unii Europejskiej do USA w kontekście produktów farmaceutycznych i wyrobów medycznych nie stanowi przekazywania danych podlegającego warunkom Tarczy Prywatności (załącznik II sekcja III pkt 14 lit. g), i). Mimo to przekazywanie danych kodowanych za pomocą klucza cieszy się ochroną na podstawie europejskich przepisów w sprawie ochrony danych. Oznacza to, że w praktyce Tarcza Prywatności nie obejmuje takich przypadków przekazywania danych. WP29 wzywa Komisję Europejską do wyraźnego zagwarantowania, że w projekt decyzji w sprawie odpowiedniej ochrony danych osobowych nie będzie obejmował przekazywania danych kodowanych za pomocą klucza w celach farmaceutycznych lub medycznych i w związku z tym, że przekazania takie objęte zostaną innymi zabezpieczeniami, np. standardowymi klauzulami umownymi (dalej: SCC) lub wiążącymi regułami korporacyjnymi (BCR). WP29 sugeruje, by zostało to wyjaśnione w ostatecznej decyzji w sprawie odpowiedniej ochrony danych osobowych.

Przekazywanie informacji do celów regulacyjnych i do celów związanych ze sprawowaniem nadzoru (załącznik II sekcja III pkt 14 lit. d)).

WP29 jest zaniepokojona tym, że na podstawie tych postanowień dane osobowe, które ze względu na kontekst medyczny mają w większości charakter wrażliwy, będą mogły być przekazywane do organów regulacyjnych w USA. Ponieważ Tarcza Prywatności ma na celu regulację przekazywania danych pomiędzy podmiotami prywatnymi, wydaje się, że organ publiczny, taki jak amerykański urząd regulacyjny, nie ma prawa dokonać samocertyfikacji na podstawie Tarczy Prywatności, co rodzi pytanie o odpowiednią ochronę danych w przypadku takiego przekazywania danych. Jeśli przekazywanie takie musi być przeprowadzone w celach regulacyjnych należy podjąć odpowiednie kroki w celu zapewnienia ciągłej ochrony praw podstawowych podmiotu danych z UE. WP29 podkreśla fakt, że projekt decyzji w sprawie odpowiedniej ochrony danych osobowych nie zawiera żadnych ustaleń w tym względzie. W związku z tym WP29 nie ma żadnych gwarancji, że dane wrażliwe podmiotów z UE będą cieszyć się w tym kontekście odpowiednią ochroną.

Dodatkowo WP29 zwraca uwagę na fakt, że nie rozumie dlaczego cel „marketing" został wymieniony jako przykład przetwarzania na potrzeby przyszłych badań naukowych. Niejasna jest także przyczyna umieszczenia sytuacji dalszego przekazywania danych do obiektów firmy i innych badaczy (załącznik II sekcja III pkt 14 lit. d)) pod nagłówkiem „Przekazywanie informacji do celów regulacyjnych i do celów związanych ze sprawowaniem nadzoru". Kwestie te wymagają wyjaśnienia w ostatecznej decyzji w sprawie odpowiedniej ochrony danych osobowych.

Monitorowanie bezpieczeństwa stosowania i skuteczności produktów (w tym sprawozdania do agencji rządowych) i monitorowanie pacjentów stosujących określone produkty lecznicze lub wyroby medyczne.

Tarcza Prywatności dopuszcza wyłączenia z obowiązywania zasad powiadomienia, wyboru, odpowiedzialności za wtórne przekazywanie danych i dostępu w zakresie, w jakim zapewnienie zgodności z tymi zasadami uniemożliwia spełnienie wymogów ustawowych. Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych nie zawiera żadnych ustaleń dotyczących sytuacji, gdy zasady prywatności negatywnie wpływają na zgodność z wymogami ustawowymi. Nawet jeśli WP29 uznaje, że dochodzenia rządowe mogą uzasadniać ograniczenia dotyczące zastosowania zasady powiadomienia i zasady dostępu w celu ochrony dochodzenia, to WP29 nie widzi przyczyn uzasadniających takie szerokie wyłączenia, gdy przetwarzania dokonuje podmiot lub osoba trzecia z sektora prywatnego. Na przykład w związku z tym, że leczenie pacjentów staje się coraz bardziej zindywidualizowane, takie szerokie wyłączenie zasad prywatności w przypadku monitorowania pacjentów stosujących określone produkty lecznicze lub wyroby medyczne. jest nie do przyjęcia ze względu na to, że ten rodzaj opieki będzie się upowszechniał. Dotyczy to także sytuacji, gdy dane wykorzystywane są przez spółki farmaceutyczne w celu monitorowania bezpieczeństwa stosowania i skuteczności produktów (badania kliniczne lub sprzedaż nowych leków).

2.2.9 Informacje dostępne publicznie

Wyłączenie stosowania zasady dostępu w przypadku informacji dostępnych publicznie i informacji przechowywanych w rejestrze publicznym (załącznik II sekcja III pkt 15 lit. d) i e)) rodzi obawy co do zakresu w jakim dana osoba fizyczna, realizując swoje prawo do dostępu, chciałaby wiedzieć, czy określony administrator przetwarza jej dane, a także wiedzieć jakie dane są przedmiotem przetwarzania, w celu kontroli nad przetwarzaniem jej danych. WP29 wielokrotnie stwierdzała, że zgodnie z prawem UE osoby, których dane dotyczą zawsze mają prawo dostępu do swoich danych, a w koniecznych wypadkach mają prawo żądać poprawienia lub usunięcia tych danych, jeśli nie były one przetwarzane zgodnie z prawem, jeżeli są niekompletne lub niedokładne, niezależnie od tego, czy takie dane osobowe zostały opublikowane[37]. Jeśli wniosek osoby fizycznej o dostęp zostanie odrzucony ze względu na fakt, że dane uzyskano z publicznie dostępnych rejestrów lub rejestrów publicznych, taka osoba fizyczna straci zdolność do kontrolowania dokładności danych oraz skontrolowania, czy dane zostały w legalny sposób upublicznione.

Tarcza Zgodności wyłącza jednak rejestry publiczne i informacje dostępne publicznie z obowiązywania zasad powiadomienia, wyboru, dostępu i odpowiedzialności za wtórne przekazywanie (załącznik II sekcja II pkt 15 lit. b)). Wyłączenia te wydają się być zbyt szerokie w porównaniu z Dyrektywą i rodzą wątpliwości dotyczące tego, że zmniejszają one między innymi możliwości osób fizycznych w zakresie kontrolowania swoich danych i ograniczania ich rozpowszechniania.

[37] Zob. WP20, s. 4

2.3 Wnioski

WP29 uważa, że władze USA oraz Komisja Europejska wprowadziły znaczne ulepszenia do komercyjnych aspektów przekazywania danych pomiędzy dwoma kontynentami. Uwzględniając powyższą analizę WP29 uważa jednak, że część handlowa Tarczy Prywatności wymaga dodatkowych wyjaśnień w wielu kwestiach. Przedmiotem troski jest na przykład brak jednoznacznej zasady w sprawie przechowywania danych. W związku z tym WP29 ma poważne obawy, czy Tarcza Prywatności może zapewnić poziom ochrony, który będzie merytorycznie równoważny względem systemu UE.

W decyzji w sprawie odpowiedniej ochrony danych osobowych należy dokładniej wyjaśnić zastosowanie zasad celowości i wyboru. Pozostaje ryzyko luk w prawie w odniesieniu do kilku zasad, w szczególności odpowiedzialności za wtórne przekazywanie, mechanizmu rozpatrywania skarg i przetwarzania danych o zasobach ludzkich i danych farmaceutycznych. Dodatkowo kwestia, w jaki sposób należy stosować zasady Tarczy Prywatności względem przetwarzających (przedstawicieli), wymaga dalszego rozwinięcia. Należy również poświęcić szczególną uwagę zagadnieniu jasnego i jednoznacznego zastosowania terminologii.

3. OCENA GWARANCJI DOTYCZĄCYCH BEZPIECZEŃSTWA NARODOWEGO ZAWARTYCH W PROJEKCIE DECYZJI W SPRAWIE ODPOWIEDNIEJ OCHRONY DANYCH OSOBOWYCH

3.1 Gwarancje i ograniczenia dotyczące organów bezpieczeństwa narodowego USA

Ingerowanie w prawa podstawowe do życia prywatnego i ochrony danych może być dopuszczalne, o ile takie zakłócenie jest uzasadnione w demokratycznym społeczeństwie. Oznacza to, że zasady prywatności nie mają charakteru bezwzględnego i możliwe są odstępstwa od nich, jednak tylko jeśli spełnione zostaną warunki odpowiednich (zasadniczych) gwarancji. Zgodnie z celem zwiększenia ochrony prywatności podmioty powinny także dążyć do pełnego i przejrzystego wdrożenia zasad, wskazując ponadto w swoich politykach ochrony prywatności przypadki, w których regularne zastosowanie będą miały wyjątki od nich dozwolone na mocy ram prawnych w USA. Z tego samego powodu w przypadku gdy zasady lub prawo amerykańskie dopuszcza taką możliwość, oczekuje się, że w miarę możliwości podmioty będą decydować się na wyższy poziom ochrony.

W załączniku II sekcja I pkt 5 stwierdza się, że „przestrzeganie zasad prywatności może być ograniczone: a) w zakresie niezbędnym w celu spełnienia wymogów bezpieczeństwa narodowego, interesu publicznego lub egzekwowania prawa; b) ustawą, rozporządzeniem rządu lub orzecznictwem, którymi nałożono sprzeczne obowiązki lub udzielono wyraźnego upoważnienia, pod warunkiem że działając na mocy jakiegokolwiek upoważnienia tego rodzaju, podmiot potrafi wykazać, że nieprzestrzeganie przez niego zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych tym upoważnieniem; lub c) jeżeli na mocy dyrektywy lub przepisów prawa państwa członkowskiego dopuszcza się wyjątki lub odstępstwa, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych okolicznościach.

Powstaje pytanie, czy odstępstwa, o których mowa w załączniku II, są uzasadnione w społeczeństwie demokratycznym. W projekcie decyzji w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności Komisja stwierdziła, że „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”[38].

Korzystając z ram wskazanych w pkt 1.2 niniejszej opinii oraz z uwzględnieniem oświadczeń władz USA i ustaleń Komisji, WP29 oceniła obecne ramy prawne i praktyki amerykańskich agencji wywiadowczych, a także warunki, w których umożliwiają one jakiekolwiek ingerencje w prawa podstawowe w odniesieniu do poszanowania życia prywatnego i ochrony danych, chronionych na mocy europejskich ram prawnych. Ocena oparta jest na analizie dyrektywy politycznej Prezydenta nr 28 (PPD-28), rozporządzenia wykonawczego nr 12333 (EO12333) oraz na innych podstawach prawnych ustanowionych przez ustawę o kontroli wywiadu (FISA - sekcja 104, sekcja 402, sekcja 215, sekcja 501 i sekcja 702). WP29 korzystała z treści załącznika VI do Tarczy Prywatności, który obejmuje pismo przygotowane przez Sekretariat Dyrektora Wywiadu Narodowego (ODNI) i dotyczące gwarancji oraz ograniczeń, które mają zastosowanie do krajowych organów bezpieczeństwa i podsumowują informacje, które zostały przekazane Komisji Europejskiej w zakresie czynności zbierania informacji w ramach rozpoznania elektronicznego.

3.2 Gwarancja A - Przetwarzanie danych powinno odbywać się zgodnie z prawem i w oparciu o czytelne, precyzyjne i dostępne zasady

Zgodnie z europejskim prawem ingerencja musi mieć miejsce zgodnie z przepisami, ustanowionymi politykami i procedurami, a także musi być wystarczająco czytelna i dostępna (z uwzględnieniem marginesu swobody udzielonego poszczególnym krajom), w celu odpowiedniego wskazania obywatelom okoliczności i warunków, w których organy publiczne mają prawo stosować środki nadzoru.[39]

WP29 zwraca uwagę na fakt, że czynności rozpoznania elektronicznego realizowane są w oparciu o dostępne ramy prawne. Wszystkie przepisy wymienione w załączniku VI (PPD-28, FISA, amerykańska ustawa w sprawie wolności (USA Freedom Act), FOIA) są dostępne online dla wszystkich (na terenie USA i poza nim). Załącznik VI zawiera podsumowanie

[38] Projekt decyzji Komisji na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA, motyw 75

[39] Europejski Trybunał Praw Człowieka, Zacharow, pkt 247 „Trybunał wcześniej uznał, że wymóg „przewidywalności" praw nie sięga tak daleko, by wymagać od państw wprowadzania przepisów prawa, które szczegółowo wskazywałyby każde postępowanie, które może spowodować wydanie decyzji o poddaniu danej osoby tajnej inwigilacji z powodów „bezpieczeństwa narodowego”. Z natury rzeczy zagrożenia dla bezpieczeństwa narodowego mogą mieć różny charakter i mogą być nieprzewidywalne lub trudne do zdefiniowania zanim wystąpią (zob. Kennedy, cyt. powyżej, pkt 159). Jednocześnie Trybunał podkreślił także, że w sprawach dotyczących praw podstawowych byłoby niezgodne z zasadą praworządności, jedną z podstawowych zasad społeczeństwa demokratycznego zapisaną w Konwencji, by uznaniowość udzielona władzy wykonawczej w sferze bezpieczeństwa narodowego miała być wyrażona w formie przymusu bezpośredniego. W związku z powyższym prawo musi wskazywać zakres takiej uznaniowości udzielonej właściwym władzom oraz sposób jej realizacji z wystarczającą jasnością, uwzględniając zgodny z prawem cel przedmiotowego środka, po to by zapewnić osobom fizycznym ochronę przed arbitralną ingerencją”.

obowiązujących ram prawnych, opisuje ograniczenia dotyczące gromadzenia danych, ich przechowywania i rozpowszechniania, kwestie zgodności z prawem i nadzoru, przejrzystości i środków prawnych. Na system prawny w USA dotyczący czynności wywiadowczych składa się szereg dokumentów, w tym sprawozdania poszczególnych agencji, polityki i procedury, które należy przeanalizować w celi lepszego rozpoznania, w jaki sposób te czynności są prowadzone zarówno w teorii jak i w praktyce. W tym zakresie WP29 skoncentrowała się na ograniczonej liczbie kwestii, które uznaje za kluczowe.

3.2.1 Rozporządzenie wykonawcze nr 12333 i dyrektywa polityczna Prezydenta nr 28

Zakres rozporządzenia wykonawczego 12333 jest szeroki. Co do zasady zbieranie informacji wywiadowczych za granicą może odbywać się według uznania prezydenta USA w oparciu o to rozporządzenie. Podnosi się jednak, że od czasu wprowadzenia FISA, rozporządzenie wykonawcze 12333 może być stosowane jedynie do zbierania danych poza terytorium USA. WP29 zwraca uwagę na fakt, że rozporządzenie wykonawcze 12333 nie zawiera wiele szczegółów dotyczących jego zakresu geograficznego, zakresu gromadzenia danych, przechowywania lub ich dalszego rozpowszechniania, ani charakteru naruszeń, które mogą dawać podstawy do nadzoru, czy rodzaju informacji, które mogą być zbierane lub wykorzystywane.

Według ustaleń WP29 głównym celem dyrektywy politycznej Prezydenta nr 28 (PPD-28) jest ustalenie granic gromadzenia i przetwarzania danych osobowych, niezależnie od stosowanego programu nadzoru i miejsca pozyskiwania danych.

PPD-28 jest dyrektywą Prezydenta Stanów Zjednoczonych, w której ustanowiono zasady spójności, na podstawie których dopuszcza się i realizuje zbieranie danych rozpoznania elektronicznego, jednak PPD-28 nie stanowi podstawy prawnej gromadzenia tych danych. PPD-28 jest skuteczna ze względu na zobowiązanie organów wywiadowczych do wdrożenia tych zasad w swoich politykach i procedurach. Dyrektywa dotyczy czynności rozpoznania elektronicznego niezależnie od lokalizacji danych w momencie ich zbierania (czy znajduje się w USA czy nie). W związku z tym dotyczy ona także danych zbieranych do celów rozpoznania elektronicznego, gdy są one przekazywane z UE do USA.

PPD-28 stanowi w szczególności, że czynności rozpoznania elektronicznego powinny być zindywidualizowane w wykonalnym stopniu.[40] W odniesieniu do wykorzystania danych dyrektywa ustanawia procedury minimalizacji danych (w tym warunki przechowywania i rozpowszechniania takich danych), bezpieczeństwa danych i dostępu do nich odpowiednich pracowników [tj. zasady zawierające gwarancje ograniczające ryzyka nadużycia i nieodpowiedniego wykorzystania], jakości danych i nadzoru. Gwarancje te mają zastosowanie niezależnie od narodowości podmiotów danych, tj. do osób fizycznych z USA i spoza USA.

[40] „Czynności rozpoznania elektronicznego powinny być zindywidualizowane w wykonalnym stopniu. W ustalaniu, czy należy zbierać informacje z rozpoznania elektronicznego Stany Zjednoczone uwzględniają dostępność innych informacji, także ze źródeł dyplomatycznych i publicznych. Należy priorytetowo traktować takie odpowiednie i wykonalne alternatywy dla rozpoznania elektronicznego". (Sekcja 1 lit. d))

W trakcie przekazywania danych do USA gwarancje ustanowione przez PPD-28 także obowiązują. Załącznik VI zawiera zobowiązanie ODNI, że jeżeli organy wywiadowcze USA miałyby zbierać dane z przewodowej komunikacji transatlantyckiej podczas ich transmisji do Stanów Zjednoczonych, „czyniłyby tak z zastrzeżeniem obowiązywania ograniczeń i gwarancji zawartych w niniejszym dokumencie, w tym wymogów PPD-28”[41]. WP29 zwraca uwagę na brak ustalonego orzecznictwa ustalającego legalność przechwytywania transmisji przewodowej przez jakiekolwiek państwo. USA ani nie potwierdzają ani nie zaprzeczają, że stosują przechwytywanie danych w transmisji przewodowej jako środek zbierania danych wywiadowczych.

Koncepcja „rozpoznania elektronicznego” nie jest zdefiniowana w PPD-28 ani innym mającym zastosowanie dokumencie.

3.2.2 Ustawa o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego

Tekst ustawy FISA w ogólnym zakresie wydaje się czytelniejszy i bardziej precyzyjny. Jednak interpretacja wielu jej przepisów w świetle PPD-28 i tym samym ich praktyczne zastosowanie w dużej mierze zależy od ich wdrożenia w poszczególnych agencjach. Pełny raport w sprawie wdrożenia nowych gwarancji nie jest jeszcze dostępny, jednak delegaci z USA poinformowali przedstawicieli WP29, że wdrożenie gwarancji z PPD-28 zostało ukończone i przebiega w podobny sposób we wszystkich organach wywiadowczych USA.

Co do szczegółów, w sekcji 501 przedstawiono względnie więcej czytelnych informacji w odniesieniu do rodzaju dopuszczanych czynności wywiadowczych: „produkcja przedmiotów materialnych (w tym książek, nagrań, gazet, dokumentów i innych rzeczy)”. Należy jednak zwrócić uwagę, że definicja „przedmiotów materialnych” obejmuje „inne rzeczy” i sprawia, że zakres tego uprawnienia jest dosyć szeroki.

W sekcji 702, na mocy której dopuszcza się zbieranie danych osób spoza USA, co do których istnieje uzasadnione przypuszczenie, że znajdują się poza USA w celu uzyskania informacji wywiadowczych za granicą,[42] nie występuje już taki poziom szczegółowości jak w sekcji 501. Co do jej zakresu, sekcja 702 zajmuje się dostawcami usług łączności elektronicznej prowadzącymi działalność w USA w zakresie zbierania za granicą informacji wywiadowczych dotyczących osób znajdujących się poza USA. Definicja „zagranicznych informacji wywiadowczych” jest szeroka. Obejmuje ona między innymi „informacje dotyczące obcego mocarstwa lub obcego terytorium, które związane są z prowadzeniem spraw zagranicznych przez Stany Zjednoczone”[43], co jest źródłem niepewności co do typu informacji, które w praktyce można zbierać.

Pomimo odtajnienia dokumentów, sprawozdań do Kongresu i sprawozdań z nadzoru Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (dalej: PCLOB), zastosowanie przepisów ustawy FISA, w tym ich zakres i zastosowanie określonych terminów

[41] Załącznik VI do Tarczy Prywatności, Biuro Dyrektora Wywiadu Narodowego (ODNI) - pismo dotyczące gwarancji i ograniczeń dotyczących organów bezpieczeństwa narodowego USA, s. 2.
[42] 50 U.S. Code, art. 1881a (D)(1)
[43] 50 U.S. Code, art. 1801 (e) (2).

umożliwiających selekcję, pozostaje niejasne i mylące. W sprawozdaniu PCLOB[44] mowa jest o wykorzystaniu określonych terminów umożliwiających selekcję („selektorów"), przy czym WP29 zakłada, że nie chodzi tu o zasady wyznaczania na podstawie sekcji 702[45]. Nie są one wspomniane w ogólnodostępnych zasadach, przynajmniej w zakresie w jakim WP29 była w stanie to stwierdzić.

3.2.3. Wniosek

Ogólnie rzecz biorąc WP29 zwraca uwagę na fakt, że mające zastosowanie dokumenty dotyczące czynności wywiadowczych są dostępne online, a także że władze USA podejmują szereg ważnych działań na rzecz przejrzystości.

WP29 docenia fakt, że od roku 2013 opublikowano dużą liczbę dokumentów, takich jak polityki, procedury, decyzje FISC i inne odtajnione dokumenty. Dodatkowo PCLOB opublikowała ważne sprawozdania dotyczące czynności prowadzonych na podstawie sekcji 702 oraz amerykańskiej ustawy o wolności. Spodziewana jest publikacja zbliżonego sprawozdania na podstawie rozporządzenia wykonawczego 12333.

Szereg załączników do dokumentów legislacyjnych, które mogłyby rzucić nieco światła na skutki rozporządzenia wykonawczego dla osób spoza USA oraz na odpowiednie gwarancje, pozostaje tajnych i niedostępnych dla opinii publicznej lub osób, na które ich zastosowanie może mieć wpływ. Teksty odtajnione mają jedynie niewielką wartość i zawierają niewiele informacji o czynnościach wywiadowczych.

Pomimo wysiłków na rzecz wyjaśnienia mechanizmów działania rozporządzenia wykonawczego 12333 po doniesieniach Snowdena, w szczególności poprzez przyjęcie PPD-28, bieżące, praktyczne zastosowanie rozporządzenia wykonawczego 12333 pozostaje niejasne. WP29 zwraca uwagę na fakt, że załącznik VI do Tarczy Prywatności nie zawiera szczegółowych informacji na temat funkcjonowania rozporządzenia wykonawczego 12333.

WP29 z zadowoleniem przyjmuje ograniczenia wprowadzone przez PPD-28, jednak ciężko jest stwierdzić, czy ramy prawne USA w zakresie nadzoru są wystarczająco przewidywalne, tj. czy zawierają „odpowiednie wskazania co do okoliczności i warunków, w których organy publiczne mają prawo stosować takie środki". Oczekiwane są dodatkowe wyjaśnienia, łącznie z publikacją sprawozdania PCLOB na temat rozporządzenia wykonawczego 12333.

3.3 Gwarancja B - należy wykazać konieczność i proporcjonalność w odniesieniu do realizowanych zgodnych z prawem celów

3.3.1 Dyrektywa Polityczna prezydenta nr 28

PPD-28 wprowadziła ograniczenia dotyczące celów, do których mogą być wykorzystywane dane osobowe i warunków pod którymi mogą być rozpowszechniane, które wpływają na

[44] Sprawozdanie PCLOB w sprawie programu nadzoru stosowanego na podstawie sekcji 702 FISA, s. 32
[45] 50 U.S. Code, art. 1881a(D)

zbieranie danych z rozpoznania elektronicznego niezależnie od zastosowanej podstawy prawnej.

W szczególności sekcja 1 PPD-28 stanowi, że czynności amerykańskiego rozpoznania elektronicznego powinny być „zindywidualizowane w wykonalnym stopniu". Uznając to ograniczenie, ciężko jest ustalić, czy „zindywidualizowane w wykonalnym stopniu" oznacza, że wszystkie czynności zbierania danych są konieczne i proporcjonalne.

PPD-28 stanowi, że masowe gromadzenie danych w dalszym ciągu jest dozwolone „w celu identyfikacji nowych lub wzrastających zagrożeń i innych informacji o kluczowym znaczeniu dla bezpieczeństwa narodowego, które często ukryte są w dużych i złożonych systemach nowoczesnej, globalnej komunikacji".[46] WP29 zwraca uwagę na fakt, że PPD-28 stanowi, że „hurtowe zbieranie danych rozpoznania elektronicznego oznacza uprawnione zbieranie dużych ilości danych z rozpoznania elektronicznego, które ze względu na uwarunkowania techniczne lub operacyjne pozyskiwane są bez stosowania kwalifikatorów (tj. specjalnych identyfikatorów, terminów umożliwiających selekcję, itd.)".

PPD-28 nakłada ograniczenia w odniesieniu do wykorzystywania danych rozpoznania elektronicznego pozyskiwanych hurtowo dotyczące celu ich wykorzystania. Jest to sześć celów, do których dane mogą być zbierane hurtowo, łącznie ze zwalczaniem terroryzmu i innych form ciężkich (międzynarodowych) przestępstw. Analiza WP29 sugeruje, że ograniczenie celu ma raczej szeroki zakres (prawdopodobnie zbyt szeroki) i nie może być uznane za odpowiednio ukierunkowane.

PPD-28 nie eliminuje możliwości hurtowego zbierania danych bez ich wcześniejszej kwalifikacji, a skala możliwości zbierania danych w ten sposób pozostaje niejasna i jest potencjalnie duża. W tym względzie WP29 zwraca uwagę na fakt, że w załączniku VI ODNI stwierdza, że „wszelkie czynności hurtowego zbierania danych dotyczące komunikacji w internecie, które realizują organy wywiadowcze USA w formie rozpoznania elektronicznego dotyczą niewielkiej części internetu"[47], w związku z czym z zadowoleniem przyjęłaby dodatkowe dowody na to w formie środków na rzecz przejrzystości.

3.3.2 Ustawa o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego

W sekcji 215 i 702 FISA wprowadzono procedury minimalizacji mające chronić osoby z USA przed daleko idącym dostępem organów władz do ich danych. Ograniczenia te oficjalnie nie mają zastosowania do cudzoziemców, mimo tego, że przedstawiciele władz USA wielokrotnie twierdzili podczas spotkań publicznych i prywatnych z przedstawicielami WP29, że zakres zastosowania procedur minimalizacji został od czasu ich wprowadzenia

[46] PPD-28, sekcja 2 i załącznik VI do Tarczy Prywatności, Biuro Dyrektora Wywiadu Narodowego (ODNI) - pismo dotyczące gwarancji i ograniczeń dotyczących organów bezpieczeństwa narodowego USA, s. 3.
[47] Załącznik VI do Tarczy Prywatności, Biuro Dyrektora Wywiadu Narodowego (ODNI) - pismo dotyczące gwarancji i ograniczeń dotyczących organów bezpieczeństwa narodowego USA, s. 4; WP29 przypomina w tym względzie sprawozdanie z ustaleniami unijnych współprzewodniczących doraźnej Grupy Roboczej UE-USA ds. ochrony danych, w którym podano, że „dane dotyczące komunikacji stanowią bardzo małą część globalnego ruchu w internecie", biorąc pod uwagę fakt, że „olbrzymia większość globalnego ruchu w internecie to duże ilości danych przesyłanych w technologii streamingu i pobrania, np. seriali telewizyjnych, filmów i transmisji sportowych" (art. 3.1.2 sprawozdania)44

rozszerzony w praktyce o wszystkie osoby, niezależnie od ich narodowości czy miejsca zamieszkania.

W sekcji 702 wskazano, że uprawnione pozyskiwanie danych „prowadzone jest w sposób zgodny z czwartą poprawką do Konstytucji Stanów Zjednoczonych z ograniczeniem zbierania danych do tego, co uważa się za zgodne z zasadą racjonalnego wyszukiwania. W tym względzie nie występują różnice między przedsiębiorstwami z USA i spoza USA". Innymi słowy pod warunkiem, że do wszystkich danych zbieranych w USA zastosowanie ma czwarta poprawka, hurtowe zbieranie danych w USA byłoby „nieracjonalne" i tym samym niekonstytucyjne.

WP29 z zadowoleniem przyjmuje ustalenia sprawozdania PCLOB, stanowiące, że „w praktyce osoby spoza USA także korzystają z ograniczeń w dostępie i przechowywaniu, wymaganych na podstawie procedur minimalizacji lub ukierunkowywania poszczególnych agencji ze względu na koszty i trudności z identyfikacją i usuwaniem informacji o osobach z USA w przypadku dużych zbiorów danych, co oznacza, że standardowo cały taki zbiór przetwarzany jest zgodnie z wyższymi standardami przetwarzania danych obowiązującymi w USA".

WP29 zwraca także uwagę na fakt, że według ustaleń PCLOB „program nie działa w formie hurtowego zbierania danych komunikacyjnych". Sprawozdanie statystyczne dotyczące przejrzystości za 2014 opublikowane przez ODNI potwierdza te ustalenia. Dodatkowo, zgodnie ze sprawozdaniem PCLOB, do ukierunkowania nadzoru służą „selektory", takie jak adres e-mail czy numer telefonu[48].

Odpowiednie dostępne publiczne zasady dotyczące ukierunkowywania nie stanowią jednak zasad takiego ukierunkowywania, a ich celem jest wyłącznie unikanie obierania jako celu osób fizycznych z USA lub posiadających miejsce pobytu w USA. Dodatkowo korzyści, które według PCLOB dostępne są dla osób fizycznych spoza USA w praktyce nie są prawnie wiążące ani ustanowione w formie aktu prawa, ponieważ dostępna legislacja dotycząca obierania celów wywiadu nie podaje jego zasad, a jej celem jest wyłącznie unikanie obierania jako celu osób fizycznych z USA lub osób posiadających miejsce pobytu w USA.

WP29 dodatkowo przypomina, że na potrzeby sekcji 702 osobami nie są tylko osoby fizyczne, lecz także grupy, podmioty, zrzeszenia, spółki kapitałowe lub zagraniczne mocarstwa. Dodatkowo fakt, że gromadzenie uzasadnione jest tym, że „znaczącym celem pozyskiwania danych jest uzyskanie zagranicznych informacji wywiadowczych" pozostawia pewną niepewność co do jego celu i konieczności. Niezależnie od tego WP29 z zadowoleniem przyjmuje informacje podane w załączniku VI, że łączna liczba osób będących przedmiotem ukierunkowywania na podstawie sekcji 702 w roku 2014 wyniosła około 90 tysięcy osób[49]. Pierwszy przegląd Tarczy Prywatności będzie szansą na zapoznanie się z dodatkowymi informacjami na temat zasad ukierunkowywania.

[48] Sprawozdanie PCLOB w sprawie programu nadzoru stosowanego na podstawie sekcji 702 FISA, s. 32
[49] Załącznik I, s. 11

Do tej pory nie powstało ostateczne orzecznictwo w sprawie legalności hurtowego zbierania danych bez rozróżnienia i późniejszego wykorzystania danych osobowych w celu zwalczania przestępczości, w tym sprawie okoliczności, w jakich takie zbieranie i wykorzystywanie danych osobowych mogłoby mieć miejsce. TSUE ma zająć się tą kwestią przynajmniej w pewnym zakresie w ciągu 2016 r. w ramach połączonych spraw Tele2 Sverige AB przeciwko Post-och telestyrelsen i Sekretarz Stanu Departamentu Spraw Wewnętrznych przeciwko Davis i inni[50], a także we wskazówkach dotyczących ważności porozumienia PNR z Kanadą[51]. W międzyczasie WP29 przypomina, że hurtowe zbieranie danych bez ich różnicowania w żadnym przypadku nie może być uznane za proporcjonalne.[52]

3.3.3. Wniosek

Pomimo ograniczeń wprowadzonych wraz z wejściem w życie PPD-28 wątpliwości WP29 nie zostały rozwiane, w szczególności w zakresie proporcjonalności zbierania danych. Po pierwsze istnieją przesłanki, by przypuszczać, że USA w dalszym ciągu zbiera dane hurtowo i bez ich kwalifikacji, a w każdym razie nie wyklucza, że będzie tak postępować w przyszłości. WP29 konsekwentnie twierdzi, że takie gromadzenie danych jest niezgodne z prawem UE i tym samym jest niedopuszczalne.

Po drugie WP29 zwraca uwagę na fakt, że także ukierunkowane przetwarzanie danych, czy też przetwarzanie, które jest „zindywidualizowane w wykonalnym stopniu" w dalszym ciągu może być uznane za prowadzone na masową skalę. To, czy zbieranie danych na masową skalę powinno zostać dopuszczone nie stanowi obecnie przedmiotu postępowania przez TSUE. Z tego względu WP29 nie dokona ostatecznej oceny legalności ukierunkowanego, lecz prowadzonego na masową skalę przetwarzania danych. WP29 podkreśla jedna, że w przypadku dopuszczenia zbierania ukierunkowanych danych na masową skalę zasady ukierunkowywania powinny dotyczyć zarówno zbierania, jak i późniejszego wykorzystania danych i nie można ich ograniczać tylko do wykorzystania takich danych. Niezależnie od powyższego konieczne jest zawarcie stosownych wyjaśnień w projekcie decyzji w sprawie odpowiedniego poziomu ochrony w związku z sześcioma celami wymienionymi w PPD-28, w przypadku których dane mogą być zbierane „hurtowo". Na tym etapie WP29 nie jest przekonana, że cele te są wystarczająco ograniczone by zapewnić, że gromadzenie danych jest rzeczywiście ograniczone do tego, co konieczne i proporcjonalne.

3.4 Gwarancja C - powinien istnieć mechanizm niezależnego nadzoru

USA nie mają jednego organu nadzoru na szczeblu federalnym, któremu powierzono by nadzór nad skutkami programów wywiadowczych i inwigilacji dla ochrony prywatności i danych osobowych. Czynności wywiadowcze USA są natomiast przedmiotem wielopoziomowego procesu nadzoru: występuje rozróżnienie pomiędzy nadzorem

[50] TSUE, połączone sprawy C-203/15 i C-698/15
[51] TSUE, sprawa A-1/15
[52] WP215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf

zewnętrznym a wewnętrznym. WP29 docenia fakt, że praktyka sprawozdawcza organów nadzoru USA jest bardzo szczegółowa i większej części dostępna publicznie.

3.4.1 Nadzór wewnętrzny

Wszystkie agencje wywiadu i bezpieczeństwa mają wyznaczonych pracowników, których zadaniem jest zapewnienie zgodności z ramami prawnymi - należą do nich także inspektorzy generalni, których podstawowym zadaniem jest ocena ogólnej zgodności prac agencji z przepisami, w tym między innymi z prawem dotyczącym ochrony prywatności i danych osobowych. Inspektorzy generalni powoływani są na mocy ustawy i są (lub wkrótce będą) mianowani przez Prezydenta po zatwierdzeniu przez Senat, co ma zapewnić, że będą organizacyjnie niezależni i odpowiadać będą przez Kongresem. WP29 uważa w związku z tym, że istnieje duże prawdopodobieństwo, że inspektorzy generalni będą spełniać kryteria organizacyjnej niezależności zgodnie z definicją opracowaną przez TSUE i Europejski Trybunał Praw Człowieka (ECtHR), przynajmniej od momentu, gdy nowy proces powoływania będzie obowiązywał ich wszystkich. W międzyczasie pozostają pewne wątpliwości co do inspektorów generalnych, których wciąż powołuje dyrektor agencji, którą nadzorują.

Inspektorzy generalni mogą sporządzać zalecenia, które mogą być następnie przekazywane do Departamentu Sprawiedliwości lub PLCOB lub nawet do komisji kongresowej, która może egzekwować ich wdrożenie. Jeżeli Inspektor generalny wykryje naruszenie, może ono być przedmiotem działań wewnętrznych lub w ramach polityki i jego wystąpienie może zostać zgłoszone Kongresowi. Inspektor generalny ma na przykład prawo przeprowadzania zarówno audytów jak i kontroli.

WP29 zwraca uwagę na fakt, że sprawozdania inspektora generalnego mogą zostać wyłączone z podawania do publicznej wiadomości, a inspektorowi generalnemu także można uniemożliwić złożenie sprawozdania, jeżeli informacja będąca przedmiotem kontroli jest tajna. Sprawozdania w każdym jednak przypadku podlegają nadzorowi ze strony Kongresu, co stanowi istotne zabezpieczenie, nawet jeżeli nie daje ona możliwości skorzystania ze środków ochrony prawnej przez osobę fizyczną.

Wszystkie agencje posiadają pełnomocników ds. prywatności i swobód obywatelskich, którzy wspierają obowiązkowy system samodzielnej sprawozdawczości w ramach nadzoru przez Kongres.

Ogólnie rzecz biorąc mechanizmy nadzoru wewnętrznego uznać można za względnie solidne; aby jednak uzasadnić ingerencję w prawa podstawowe do ochrony prywatności i danych osobowych, nadzór musi być w pełni niezależny. Mimo tego, że WP29 szanuje i docenia pracę pełnomocników ds. prywatności i swobód obywatelskich, nie może stwierdzić, że osiągają oni wymagany próg niezależności wymagany od niezależnych nadzorców.

3.4.2 Nadzór zewnętrzny

Nadzór zewnętrzny składa się z szeregu mechanizmów: nadzór sądowy na postawie sekcji 501 i 702 zapewniany jest przez Trybunał FISA (zwany dalej: FISC), nadzór ze strony kongresowych komisji specjalnych ds. wywiadu, a także zadania realizowane przez PCLOB.

WP29 przypomina, że w idealnej sytuacji, jak stwierdził to TSUE oraz ECtHR, nadzór powinien znajdować się w rękach sędziego, co gwarantowałoby niezależność i bezstronność postępowania. Do niedawna postępowanie FISC było postępowaniem ex parte, bez możliwości skorzystania przez osobę fizyczną z prawa do bycia wysłuchanym, lub nawet bez jej informowania o toczącej się sprawie. Także teraz postępowanie FISC pozostaje postępowaniem ex parte, jednak po przyjęciu amerykańskiej Ustawy o wolności do FISC wprowadzono instytucję amici curiae. Osoba działająca tym charakterze działa niezależnie, ale nie jest powoływana do obrony konkretnych osób fizycznych, które mogą występować w danej sprawie.

Na mocy amerykańskiej ustawy o wolności powołano grupę osób działających jako amici curiae, które mają przekazać FISC informacje o istotnych sprawach. Trybunał wybrał pięciu prawników, którzy otrzymali odpowiednie certyfikaty bezpieczeństwa i porady techniczne, uczestniczą w rozprawach przed FISC i przekazują streszczenia spraw, a także prowadzą argumentację merytoryczną dotyczącą danej sprawy z punktu widzenia prywatności i praw obywatelskich. Czynią tak jednak wyłącznie w istotnych sprawach lub gdy pojawiają się nowe pytania prawne.[53]

Sekcja 215 niemal w całości podlega nadzorowi sądowemu ex ante (ale nie ex post), ponieważ wszystkie programy korzystające z sekcji 215 jako podstawy do zbierania danych wymagają zgody ze strony FISC. W sprawozdaniu PCLOB wskazano, że „sekcja 702 różni się od tradycyjnych ram wywiadu elektronicznego FISA zarówno pod względem zastosowanych standardów, jak i braku indywidualnych ustaleń wykonywanych przez FISC. Na podstawie ustawy Prokurator Generalny i Dyrektor Wywiadu Narodowego dokonują rocznych certyfikacji zezwalających na ukierunkowywanie nadzoru na osoby spoza USA, co do których istnieją racjonalne przesłanki by przypuszczać, że znajdują się poza USA, w celu zebrania zagranicznych informacji wywiadowczych, bez podawania FISC szczegółowych danych na temat osób spoza USA, które będą objęte takimi czynnościami. [...] Brak jest również wymogu, by władze wykazały prawdopodobną przyczynę stwierdzenia, że cel nadzoru na podstawie sekcji 702 jest obcym mocarstwem lub przedstawicielem obcego mocarstwa, czego wymaga pierwotna wersja FISA”.[54]

W Kongresie nadzór w zakresie zatwierdzania czynności wywiadowczych, w szczególności w formie głosowania nad budżetem, sprawują komisje specjalne ds. wywiadu. Komisje ds. wywiadu Senatu i Izby Reprezentantów otrzymują tajne podsumowania czynności wywiadowczych. AG musi składać co pół roku składać tym komisjom sprawozdania

[53] Ustawa o wolności - tytuł IV - Reformy trybunałów ds. zagranicznych informacji wywiadowczych - Sekcja 401 Powołanie amici curiae
[54] Sprawozdanie PCLOB w sprawie programu inwigilacji stosowanego na podstawie sekcji 702 FISA, s. 24, 25

dotyczące wywiadu elektronicznego FISA. Niejasne pozostaje dla WP29, w jakim zakresie są one w stanie omawiać przetwarzanie danych osobowych osób fizycznych, szczególnie spoza USA.

PCLOB jest niezależną instytucją władzy wykonawczej w USA, której powierzono dwa podstawowe zadania: (1) przegląd i analizę działań władzy wykonawczej w celu ochrony narodu [amerykańskiego] przed terroryzmem, z uwzględnieniem faktu, że potrzeba prowadzenia takich działań bilansowana jest koniecznością ochrony prywatności i wolności obywatelskich, oraz (2) zapewnienie, by kwestie dotyczące wolności były odpowiednio uwzględniane w trakcie opracowywania i wdrażania przepisów, regulacji i polityk związanych z działaniami na rzecz ochrony społeczeństwa przed terroryzmem. WP29 zwraca także uwagę na fakt, że PCLOB ma prawo do żądania stawiennictwa i dostęp do informacji tajnych. W ramach realizacji swoich zadań sprawdza także skuteczność programów. Jej nadzór realizowany jest po zdarzeniu, a nie przed jego wystąpieniem. PCLOB wykazała niezależność w działaniu odrzucając argumentację Prezydenta Stanów Zjednoczonych w kwestiach prawnych. W szczególności uznała, że program dotyczący metadanych telefonicznych na podstawie sekcji 215 nie został zgodnie z prawem dopuszczony i wskazała, że nie był skuteczny, ponieważ nie było dowodów na niszczące ataki. PLCOB przeprowadziła także roczne badanie programu na podstawie sekcji 702 i stwierdziła, że jest zgodny z prawem i jednoznacznie dopuszczony na mocy ustawy, oraz że sekcja 702 wykazała dużą skuteczność, także w kwestiach związanych z terroryzmem. Działała ona zgodnie z wymogiem przejrzystości i ustaliła, że nie istniała potrzeba utajniania części tajnych faktów. W najbliższej przyszłości PCLOB ma opublikować sprawozdanie z wdrożenia PPD-28. W tym względzie stwierdza ona, że sam fakt, że dana osoba jest obcokrajowcem nie stanowi podstawy do przechowywania informacji o niej.

WP29 zwraca wreszcie uwagę na fakt, że rozporządzenie wykonawcze 12333 nie przewiduje mechanizmów przeglądu sądowego, nadzoru lub ochrony prawnej w odniesieniu do programów inwigilacji prowadzonych na jego podstawie.

3.4.3. Wniosek

Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych wskazuje, że w USA obowiązuje wielopoziomowe podejście do mechanizmów kontroli zewnętrznej i wewnętrznej. Mimo tego, że mechanizmy funkcjonowania nadzoru mogą być mylące, WP29 jest przekonana, że co do zasady ustanowiono wystarczającą liczbę mechanizmów nadzoru wewnętrznego. WP29 obawia się jednak, że nadzór nad programami inwigilacji realizowanymi na podstawie rozporządzenia wykonawczego 12333 jest niewystarczający.

WP29 zwraca uwagę na fakt, że jej poprzednia uwaga dotycząca faktu, że procedury przed FISC nie mają charakteru kontradyktoryjnego została jedynie w pewnym stopniu uwzględniona za pomocą wprowadzenia instytucji amici curiae, których zadaniem jest „zwiększanie ochrony prywatności i wolności obywatelskich osób fizycznych”. Niezależnie od tego FISC nie oferuje skutecznego nadzoru sądowego w zakresie ukierunkowywania nadzoru na osoby spoza USA. Pozostają także pewne wątpliwości co do możliwości

skutecznej oceny przez FISC procedur ukierunkowywania i minimalizacji, co zostało także wskazane przez PCLOB[55].

3.5 Gwarancja D - Osoby fizyczne powinny mieć dostęp do skutecznych środków prawnych

3.5.1 Sądowe środki zaskarżenia

3.5.1.1 Wymóg stały

System amerykański w odniesieniu do środków zaskarżenia zawiera istotne ograniczenie: Konstytucja USA wymaga od osób fizycznych wykazania prawa do dochodzenia roszczeń: „wymóg doznania przez powoda, w przeszłości lub przyszłości, bezpośredniej szkody lub uszczerbku, który podlega zadośćuczynieniu. Na szczeblu federalnym nie można wszcząć postępowania tylko dlatego, że osoba fizyczna lub grupa osób jest niezadowolona z działań władz lub przepisów".[56] Wymóg taki unieważnia brak zawiadomienia osób objętych inwigilacją także po zakończeniu stosowania tego środka. TSUE i Europejski Trybunał Praw Człowieka wielokrotnie stwierdzały, że osoby fizyczne muszą mieć dostęp do administracyjnych lub sądowych środków zaskarżenia. Europejski Trybunał Praw Człowieka potwierdził w decyzji w sprawie Zacharowa, że w oparciu o istniejące orzecznictwo każda osoba może skierować sprawę do sądu, jeśli ma uzasadnione powody by przypuszczać, iż miało miejsce naruszenie jej praw podstawowych.[57]

Dodatkowo obcokrajowcy znajdujący się poza USA nie otrzymują pełnej konstytucyjnej ochrony USA na podstawie orzecznictwa Sądu Najwyższego Stanów Zjednoczonych[58]. Dzieje się tak w szczególności w odniesieniu do czwartej poprawki, która chroni obywateli USA, lecz nie osoby spoza USA, przed nieuzasadnionym przeszukaniem i zajęciem, i z której wyprowadzana jest większość amerykańskich praw do prywatności. Obywatele UE i inne osoby z Europy mieszkające poza USA są po prostu wyłączone z zakresu ochrony na podstawie czwartej poprawki.[59]

Ograniczone zastosowanie ustawy o sądowych środkach odwoławczych (zarówno w zakresie treści, ponieważ wyłącza ona bezpieczeństwo narodowe, jak i w odniesieniu do osób, które mogą z niej skorzystać), wiele wyłączeń i niepewność prawa dotycząca agencji, wobec których obowiązywać ma ustawa o sądowych środkach odwoławczych nie spełniają warunku oferowania skutecznego mechanizmu sądowego dochodzenia roszczeń wszystkim osobom fizycznym, których dotyczą sprawy inwigilacji wywiadowczej na potrzeby bezpieczeństwa narodowego.

[55] Sprawozdanie PCLOB w sprawie programu inwigilacji stosowanego na podstawie sekcji 702 FISA, s. 11
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper przeciwko Amnesty International USA
[57] Europejski Trybunał Praw Człowieka, Zacharow, pkt 171
[58] USA przeciwko Verdugo - Urquidez, s. 264-266
[59] Sprawozdanie współprzewodniczących UE, punkt 2

3.5.1.2 Dyrektywa polityczna Prezydenta nr 28

WP29 zwraca uwagę na fakt, że PPD-28 jest jedynie dyrektywą i w związku z tym nie tworzy praw osób fizycznych. Ustanawiać je mogą tylko akty ustawodawcze. Oznacza to, że osoby fizyczne nie mogą wytaczać powództw na podstawie domniemanego naruszenia gwarancji PPD-28.

3.5.1.3 Ustawa o kontroli wywiadu przez Agencję Bezpieczeństwa Narodowego

FISA przewiduje pewne środki ochrony prawnej dla osób fizycznych w przypadku niezgodnej z prawem inwigilacji. Według FISA „osoba, która doznała szkody, inna niż, odpowiednio, mocarstwo zewnętrzne lub przedstawiciel mocarstwa zewnętrznego [...], która została poddana inwigilacji elektronicznej, lub informacje o niej pozyskane w drodze inwigilacji elektronicznej zostały ujawnione lub wykorzystane z naruszeniem sekcji 1809 niniejszego tytułu ma podstawy wystąpienia z powództwem przeciwko osobie popełniającej takie naruszenie". Postanowienie to wyłącza jednak mocarstwa zewnętrzne lub przedstawiciela mocarstwa zewnętrznego poddanego takiemu środkowi. Jednak jak już wskazano, powód musi wykazać prawo do dochodzenia roszczeń, co w praktyce nie będzie możliwe.

Amerykańska ustawa o wolności ustanowiła instytucję rady doradczej Amicus Curiae Trybunału FISA, która może, ale nie musi udzielać porad w przypadku istotnej nowej interpretacji prawa. Zadaniem jej członków jest jednak oferowanie bezstronnych porad, a nie obrona interesu określonej osoby fizycznej na jej wniosek.

3.5.2 Administracyjne środki zaskarżenia

3.5.2.1 Generalni inspektorzy

Innym trybem korzystania ze środków zaskarżenia jest zwrócenie się ze skargą do generalnego inspektora. Generalny inspektor nie ma jednak obowiązku rozpatrywania każdej skargi, nie istnieje bowiem prawo do bycia wysłuchanym, a uprawnienie w tym zakresie przysługujące generalnemu inspektorowi zależy wyłącznie od jego decyzji. Generalny inspektor może także publikować sprawozdania z ustaleniami w sprawie naruszeń, w których informacje są odtajniane. Jeżeli dana osoba fizyczna mogłaby przypuszczać, że sprawozdanie jej dotyczy, mogłaby wnieść powództwo na podstawie ustalenia naruszenia prawa.

3.5.2.2 Ustawa o wolności informacji

Środkiem zaskarżenia dostępnym dla wszystkich osób jest złożenie wniosku w sprawie wolności informacji na podstawie ustawy o wolności informacji (FOIA). Według władz USA wniosek FOIA złożyć może ogólnie rzecz biorąc każda osoba będąca lub niebędąca obywatelem USA, występująca o udostępnienie rejestrów danej agencji. Obejmuje to rejestry dotyczących osób, choć w takim przypadku konieczne jest potwierdzenie tożsamości. Jeśli jednak informacje zostały utajnione w celu ochrony bezpieczeństwa narodowego, wniosek FOIA raczej nie zostanie rozpatrzony pozytywnie, ponieważ obowiązuje wyłączenie w tym

zakresie - agencje nie muszą udostępniać informacji niejawnych, także wtedy, gdy informacje dotyczą wnioskującej o nie osoby. Informacje z trwających dochodzeń w ramach egzekwowania prawa są całkowicie wyłączone z zakresu wniosków FOIA. WP29 uważa również, że wniosek FOIA nie udziela prawa do sprawdzenia legalności przetwarzania przez niezależny organ.

3.5.3 Rzecznik ds. Tarczy Prywatności

3.5.3.1 Powołanie Rzecznika

Tarcza Prywatności ustanawia nowy mechanizm dla osób fizycznych z UE, pozwalający składać wnioski dotyczące „rozpoznania elektronicznego USA" do nowo utworzonego urzędu Rzecznika ds. Tarczy Prywatności. Na stanowisko Rzecznika, co wyjaśnia memorandum załączone do pisma sekretarza stanu Johna Kerry z dnia 22 lutego 2016 r., powołana zostanie podsekretarz C. Novelli. Będzie ona pełnić tę funkcję razem z funkcją „starszej koordynator ds. ds. międzynarodowej dyplomacji w dziedzinie technologii informacyjnej", utworzoną na mocy sekcji 4 lit. d) PPD-28. W piśmie i memorandum do niego podkreśla się, że „podsekretarz odpowiada bezpośrednio przed sekretarzem stanu i działa niezależnie od Wspólnoty Wywiadowczej".

Pomimo nazwy stanowiska, w memorandum wyjaśniono, że Rzecznik ds. Tarczy Prywatności będzie nie tylko rozpatrywał wnioski dotyczące dostępu na potrzeby bezpieczeństwa narodowego do danych przesyłanych z UE do US na podstawie Tarczy Prywatności, lecz także wnioski w zakresie danych przekazywanych na podstawie standardowych klauzul umownych, wiążących reguł korporacyjnych, odstępstw (na podstawie art. 26 dyrektywy 95/46/WE) lub „potencjalnych przyszłych odstępstw", zdefiniowanych w przypisie 2 do memorandum.

Sposób działania tego mechanizmu można podsumować w następujący sposób: osoba fizyczna z UE składa wniosek do organu państwa członkowskiego odpowiadającego za nadzór nad służbami bezpieczeństwa narodowego, lub do „organu rozpatrującego skargi obywateli Unii", w przypadku, gdyby został on utworzony lub wyznaczony. Organ przekazujący wniosek Rzecznikowi będzie musiał najpierw sprawdzić, czy wniosek jest kompletny zgodnie z pkt 3 lit. b) pisma.[60] Po przekazaniu do Rzecznika ds. Tarczy Prywatności i stwierdzeniu zgodności z pkt 3 lit. b) Rzecznik ds. Tarczy Prywatności przygotuje odpowiedź, co oznacza, że ostatecznie potwierdzi, że „(i) skarga została właściwie

[60] b. Unijny organ rozpatrujący skargi osób fizycznych zapewni kompletność wniosku poprzez poniższe działania:
(i) sprawdzenie tożsamości osoby fizycznej oraz czy dana osoba działa we własnym imieniu czy jako przedstawiciel organizacji rządowej lub międzyrządowej;
(ii) upewnienie się, że wniosek złożono w formie pisemnej i zawiera on następujące informacje podstawowe:
• wszelkie informacje, które stanowią podstawę wniosku,
• charakter informacji lub opis żądania,
• ewentualnie jednostki rządu Stanów Zjednoczonych, które uznaje się za zaangażowane, oraz
• pozostałe środki podjęte w celu uzyskania informacji lub opis żądania oraz odpowiedź otrzymana w następstwie zastosowania tych środków.
(iii) sprawdzenie, czy wniosek dotyczy danych, w przypadku których można racjonalnie założyć, że zostały przekazane Stanom Zjednoczonym przez UE zgodnie z Tarczą Prywatności, standardowymi klauzulami umownymi, wiążącymi regułami korporacyjnymi, odstępstwami lub możliwymi przyszłymi odstępstwami.
(iv) Wstępne określenie, czy wniosek nie jest niepoważny, złożony w celu nękania lub w złej wierze.

zbadana oraz że (ii) działano zgodnie z przepisami, ustawami, rozporządzeniami wykonawczymi, dyrektywami prezydenckimi i politykami agencji zawierającymi ograniczenia i gwarancje opisane w piśmie Urzędu Dyrektora Krajowych Służb Wywiadowczych (ODNI), a w przypadku nieprzestrzegania tych regulacji problem ten został rozwiązany".[61] Odpowiedź Rzecznika ds. Tarczy Prywatności „nie potwierdzi, ani nie zaprzeczy, że dana osoba jest objęta obserwacją, ani nie potwierdzi, że zastosowano specjalne środki zaradcze".[62] Co do pytania w jaki sposób prowadzone jest przez Rzecznika dochodzenie, wyjaśniono, że Rzecznik ds. Tarczy Prywatności „będzie ściśle współpracował z innymi urzędnikami rządu Stanów Zjednoczonych, w tym odpowiednimi niezależnymi organami nadzoru"[63], a konkretnie „będzie mógł ściśle współpracować z Urzędem Dyrektora Krajowych Służb Wywiadowczych, Departamentem Sprawiedliwości oraz innymi departamentami i agencjami zaangażowanymi w razie potrzeby w ochronę bezpieczeństwa narodowego Stanów Zjednoczonych oraz Inspektorami Generalnymi, urzędnikami ds. ustawy o dostępie do informacji publicznej oraz urzędnikami Biura Wolności Obywatelskich i Ochrony Prywatności"[64]. Koordynacja ma zapewniać, że Rzecznik ds. Tarczy Prywatności będzie mógł wysłać odpowiedź, a także potwierdzenia wspomniane powyżej.

3.5.3.2 Ocena nowej instytucji Rzecznika

Grupa Robocza docenia wysiłki poczynione przez Komisję Europejską i rząd USA na rzecz wprowadzenia nowego mechanizmu z zamiarem ulepszenia możliwości stosowania środków ochrony prawnej dotyczących inwigilacji przez USA. Grupa zakłada, że ocena tego mechanizmu, będącego novum w stosunkach międzynarodowych w zakresie rozpoznania elektronicznego lub bezpieczeństwa narodowego, ma szczególne znaczenie.

W tym punkcie WP29 dokona analizy, w jaki sposób powołanie Rzecznika ds. Tarczy Prywatności wiąże się z niezbędnymi wymaganiami zapewnienia osobom fizycznym możliwości stosowania środków ochrony prawnej wskazanych w Karcie, w EKPC i orzecznictwie europejskich sądów.

3.5.3.3 Czy samo powołanie Rzecznika jest wystarczające?

Przede wszystkim należy zadać sobie pytanie, czy powołanie „rzecznika" można uznać za zgodne z art. 47 Karty, który mówi o prawie do skutecznego środka ochrony prawnej przed bezstronnym sądem[65] – przynajmniej wtedy, gdy nie jest dostępna inna ścieżka dochodzenia roszczeń prawnych. Jest to istotne, ponieważ TSUE w sprawie Schrems, w istotnym punkcie 95 odnosi się do art. 47 Karty bez wskazywania, że art. 47 należy interpretować z uwzględnieniem modyfikacji w kontekście środków nadzoru. Z drugiej strony TSUE już

[61] Załącznik III do Tarczy Prywatności, sekcja 4 lit. e)
[62] Załącznik III do Tarczy Prywatności, sekcja 4 lit. e)
[63] Załącznik III do Tarczy Prywatności, sekcja 2 lit. a)
[64] Załącznik III do Tarczy Prywatności, sekcja 2 lit. a)
[65] W objaśnieniach do Karty praw podstawowych mowa jest także o tym, że art. 47 należy interpretować w taki sposób, że oferuje gwarancję obowiązywania prawa do prawo do skutecznego środka prawnego przed sądem (objaśnienia dotyczące Karty praw podstawowych, objaśnienia do art. 47 (2007/C 303/02).

zastosował art. 47 Karty w sprawie Kadi II[66] względem środków nadzoru dotyczących, odpowiednio, bezpieczeństwa narodowego i międzynarodowego[67].

Orzecznictwo Europejskiego Trybunału Praw Człowieka wyraźnie wskazuje jednak, że środki ochrony prawnej w sądach powszechnych nie stanowią warunku uznania programu inwigilacji za zgodny z art. 8 (i art. 13 EKPC).[68] Zamiast tego sąd ustalił na podstawie art. 8, że konieczną gwarancją dotyczącą czynności inwigilacji jest dostęp do środków ochrony prawnej także przed innymi organami. Europejski Trybunał Praw Człowieka ma jednak duże oczekiwania względem oferowania skutecznej ochrony prawnej przez pozostałe organy, wskazując, że organ taki musi być „niezależny od organów prowadzących inwigilację i należy powierzyć mu wystarczające uprawnienia i kompetencje, by mógł sprawować skuteczną i ciągłą kontrolę"[69].

W sprawach Kennedy i Klass Europejski Trybunał Praw Człowieka przeanalizował, co te oczekiwania mogą oznaczać w kontekście tajnej inwigilacji, gdy podmiot danych nie jest informowany o przetwarzaniu jego danych. W obu tych wyrokach organy były uznawane przez Europejski Trybunał Praw Człowieka za niezależne, w szczególności niezależne od organów prowadzących inwigilację, lecz także niezależne od poleceń[70] innych organów. Co do sprawy Kennedy, Trybunał stwierdził istnienie niezależnego i bezstronnego organu, który przyjął własny regulamin i składał się z członków piastujących wówczas lub wcześniej wysokie stanowiska w sądownictwie lub posiadających duże doświadczenie jako prawnicy[71].

Rozpatrując skargi od osób fizycznych organy w obu tych wyrokach miały także dostęp do wszystkich stosownych informacji, w tym do materiałów utajnionych. Oba z nich miały również możliwość usunięcia niezgodności.[72]

Oprócz pytania, czy Rzecznik może być uznany za „trybunał", zastosowanie art. 47 ust. 2 Karty niesie ze sobą kolejne wyzwanie, ponieważ w przepisie tym stwierdza się, że trybunał musi być „ustanowiony z mocy prawa". Wątpliwe jest, czy memorandum opisujące funkcjonowanie nowego mechanizmu może być uznane za „prawo".

W związku z tym, z uwzględnieniem zasady zasadniczej równoważności, bez analizowania, czy Rzecznik może być formalnie uznany za trybunał ustanowiony z mocy prawa, Grupa Robocza zdecydowała się omówić bardziej szczegółowo niuanse orzecznictwa w odniesieniu do określonych wymagań, których spełnienie jest wymagane dla uznania „środków ochrony

[66] Połączone sprawy C-584/10 P, C-593/10 P oraz C-595/10 P, Komisja Europejska i Wielka Brytania przeciwko Kadi, 18 lipca 2013 r.
[67] Kadi II pkt 97 i 100: wszystkie akty unijne, w tym te, które mają nadać moc uchwałom przyjętym przez Radę Bezpieczeństwa na podstawie rozdziału VII Karty Narodów Zjednoczonych, podlegają przeglądowi zgodności z prawem, prowadzonemu przez sądy Unii Europejskiej (rozdział VIII dotyczy działań w przypadku zagrożenia pokoju, naruszenia go i aktów agresji).
[68] Art. 13 EKPC zobowiązuje państwa członkowskie do zapewnienia, by „Każdy, czyje prawa i wolności […] zostały naruszone, ma prawo do skutecznego środka odwoławczego do właściwego organu państwowego". Nie musi to być organ sądownictwa, co Europejski Trybunał Praw Człowieka wyjaśnił w sprawie Klass, Art. 56 i 67.
69 Klass, pkt 56 i 67.
[70] Europejski Trybunał Praw Człowieka, Klass, pkt 21 i 53.
[71] Komisja G-10 (w czasie wyroku) składa się z trzech członków, a jej przewodniczącym musi być osoba posiadająca kwalifikacje do sprawowania urzędu sądowego, Klass pkt 21 i 53).
[72] Europejski Trybunał Praw Człowieka, Kennedy, pkt 167. Klass, Art. 21 i 53.

prawnej" i „środków zaskarżenia" za zgodne z prawami podstawowymi na podstawie art. 7, 8 i 47 Karty i art. 8 (oraz 13) EKPC. W swojej dalszej analizie, po omówieniu zakresu zastosowania nowego mechanizmu, Grupa Robocza skupi się na następujących kryteriach: wymóg zgłoszenia wniosku do Rzecznika i otrzymania odpowiedzi (stanowisko), niezależność Rzecznika, jego uprawnienia w zakresie dochodzenia i dostępu do koniecznych materiałów, w tym dokumentów niejawnych, oraz wnioskowania o pomoc z innych agencji, i wreszcie uprawnienie do wyeliminowania braku zgodności.

3.5.3.4 Zakres zastosowania instytucji Rzecznika

W odniesieniu do dostępu do instytucji rzecznika WP29 uważa, że wszystkie osoby podlegające prawu UE powinny być objęte gwarancjami na podstawie Tarczy Prywatności. Nie do zaakceptowania jest tworzenie podziałów na podstawie narodowości, szczególnie ze względu na to, że prawa podstawowe w UE udzielane są wszystkim, a nie tylko osobom posiadającym paszport UE. Załącznik III mówi o „osobach fizycznych z Unii Europejskiej" bez dalszego definiowania, kim te osoby są. Grupa Robocza wyraża rozczarowanie niejasnością tej definicji i sugeruje wprowadzenie wyjaśnienia, że wszystkie osoby podlegające przepisom UE mają prawo do rozpatrzenia ich wniosku do Rzecznika zgodnie z warunkami memorandum. Dodatkowo Komisja oraz USA powinny zająć się kwestią, w jakim stopniu Tarcza Prywatności będzie dotyczyć także obywateli/rezydentów państw EOG i Szwajcarii, którzy w przeszłości byli objęci programem „bezpieczna przystań".

Dodatkowo WP29 zwraca uwagę na pewną niejasność co do zakresu zastosowania instytucji Rzecznika. Memorandum stanowi, że zadaniem Rzecznika jest obsługa wniosków dotyczących dostępu ze względów bezpieczeństwa narodowego do danych przekazywanych Stanom Zjednoczonym przez Unię Europejską zgodnie ze wszystkimi mechanizmami przekazywania przewidzianymi prawem UE, lecz jednocześnie stanowi wyraźnie, że memorandum ustanawia ten mechanizm „w odniesieniu do rozpoznania elektronicznego". Ten ostatni termin sugeruje, że obejmuje on wyłącznie przekazywanie danych zebranych za pomocą środków rozpoznania elektronicznego, co rodzi pytanie, czy dane zebrane na podstawie FISA są uznawane za „rozpoznanie elektroniczne". Wydaje się, że sytuacja taka ma miejsce w odniesieniu do sekcji 702, co wyjaśnia oświadczenie ODNI, s. 10[73]. WP29 ubolewa jednak, że użycie terminu „rozpoznanie elektroniczne" tworzy niepotrzebną niepewność w tym kontekście.

Kolejnym skutkiem jest to, że zgodnie z interpretacją Grupy Roboczej instytucja Rzecznika nie dotyczy wniosków związanych z dostępem organów egzekwowania prawa.[74] Jeśli tak, pozostaje niejasne, czy mechanizm obejmować ma wnioski ze strony niektórych agencji, przede wszystkim CIA.

[73] Załącznik VI do Tarczy Prywatności, s. 10;
[74] Memorandum w sprawie ustanowienia Rzecznika, s. 1

3.5.3.5 „Interes prawny" i procedura wnioskowania

Wszczęcie postępowania przeciwko środkom inwigilacji ze strony rządu USA przed sądem powszechnym w USA jest niezwykle trudne. Grupa Robocza zdaje sobie sprawę, że Sąd Najwyższy nie uznawał interesu prawnego w sprawach dotyczących czynności wywiadowczych, gdy wnioskodawca nie był w stanie wykazać indywidualnej „konkretnej, uszczegółowionej, faktycznej lub nieuchronnej szkody".[75] W tym względzie ustanowienie Rzecznika jest istotnym krokiem, ponieważ dodaje nową ścieżkę dochodzenia roszczeń, która w innej sytuacji nie istniałaby. Grupa Robocza tym samym z zadowoleniem przyjmuje wyjaśnienia w pkt 3 lit. c). W oparciu o ten punkt wykazanie, że dostęp do danych wnioskującego nastąpił w następstwie czynności rozpoznania elektronicznego, nie jest niezbędne w celu złożenia wniosku na podstawie tego mechanizmu.

Grupa Robocza w dużej mierze popiera procedurę identyfikacji skarżącego na podstawie mechanizmu Rzecznika. Idealnym rozwiązaniem jest to, że identyfikacja odbywa się na terytorium UE, jak to ma miejsce w przypadku mechanizmu w sprawie dostępu na podstawie umowy TFTP2 UE-USA. Grupa Robocza nie rozumie jednak dlaczego weryfikacja w UE powinna być prowadzona przez „organy państw członkowskich odpowiedzialne za nadzór nad służbami bezpieczeństwa narodowego". Po pierwsze jest mało prawdopodobne, że w związku z art. 4 ust. 2 Traktatu o Unii Europejskiej Komisja Europejska mogłaby przypisać zadania tym organom, które jednoznacznie podlegają kompetencjom państw członkowskich.

Dodatkowo, biorąc pod uwagę różnorodność mechanizmów nadzoru służb bezpieczeństwa narodowego w państwach członkowskich, udział tych organów może znacząco wpłynąć na skuteczność systemu w państwach członkowskich z punktu widzenia obywateli. Na przykład w sytuacji, gdy zadania nadzoru nad służbami bezpieczeństwa narodowego realizuje kilka organów, zidentyfikowanie właściwego może stanowić trudność dla osoby fizycznej, jeżeli mające zastosowanie krajowe przepisy nie przewidują możliwości kontaktowania się osób fizycznych z odpowiednimi organami nadzoru, lub jeżeli organy te nie są odpowiednio przygotowane do tego, by realizować zadania narzucone im przez projekt decyzji w sprawie odpowiedniej ochrony danych osobowych[76]. Uwzględniając udział organów ochrony danych osobowych w stosowaniu Tarczy Prywatności i nadzorze nad nią, a także podobną ich rolę w umowie TFTP2, większy sens ma przypisanie tego zadania krajowym organom ochrony danych w państwa członkowskich. Grupa Robocza podkreśla, że uważa za mało prawdopodobne, by informacje niejawne były przetwarzane w ramach procedury przed Rzecznikiem ds. Tarczy Prywatności, ponieważ odpowiedź będzie mogła brzmieć „zgodne" lub „niezgodne - naprawiono".

3.5.3.6 Niezależność

Z oświadczeń sekretarza stanu jasno wynika, że stanowisko Rzecznika piastować będzie podsekretarz Departamentu Stanu. Osoba ta jest nominowana przez Prezydenta, a jej

[75] Clapper przeciwko Amnesty International USA, 568 U.S. ___ (2013) II. s. 10

[76] W niektórych państwach członkowskich na przykład osoby fizyczny mogą uzyskać dostęp do informacji w posiadaniu służb bezpieczeństwa narodowego wyłącznie w formie wniosku do sądu wyższej instancji.

nominacja wymaga zatwierdzenia przez Senat. Stanowisko Rzecznika nie wymaga dodatkowego zatwierdzenia; wystarczy powołanie do roli Rzecznika. Podsekretarz powoływany jest przez Prezydenta USA na wniosek Sekretarza Stanu na stanowisko Rzecznika i zatwierdzany w roli Podsekretarza Stanu przez Senat Stanów Zjednoczonych. W piśmie i memorandum podkreślono, że Rzecznik jest „niezależny od Wspólnoty Wywiadowczej Stanów Zjednoczonych". WP29 zastanawia się jednak, czy stanowisko Rzecznika powstaje w najbardziej odpowiednim departamencie. Pewna wiedza i znajomość mechanizmów funkcjonowania wspólnoty wywiadowczej wydaje się konieczna do skutecznej realizacji obowiązków Rzecznika, a jednocześnie niezbędne jest pewne oddalenie od wspólnoty wywiadowczej, by możliwe było niezależne działanie.

Tarcza Prywatności nie ustanawia konkretnych kryteriów odwołania Rzecznika. W związku z tym Grupa Robocza zakłada, że Rzecznika można odwołać ze stanowiska w taki sam sposób, jak odwołuje się go z funkcji podsekretarza stanu w Departamencie Stanu, co może potencjalnie negatywnie wpływać na niezależność stanowiska Rzecznika.

Na pierwszy rzut oka wyznaczenie na Rzecznika Podsekretarza Stanu w Departamencie Stanu jednoznacznie różni się – jeśli chodzi o niezależność – od ustanowienia sądu powszechnego jako sądu właściwego do dochodzenia środków ochrony prawnej przysługujących osobie fizycznej. Pytanie brzmi, czy Rzecznik może być traktowany pod względem niezależności na równi z innymi niezależnymi organami nadzoru, które zostały uznane za zgodne. W kontekście inwigilacji byłyby to w szczególności Trybunał Dochodzeniowy (IPT) w Wielkiej Brytanii oraz Komisja G10 w Niemczech.

Należy dodatkowo ocenić, czy tak rzeczywiście jest, analizując uprawnienia udzielone „niezależnym organom".

3.5.3.7 Uprawnienia dochodzeniowe

W sprawie Kadi II TSUE orzekł w odniesieniu do art. 47 Karty, by „zainteresowany miał możliwość zapoznania się z powodami decyzji wydanej w stosunku do niego, czy to za pomocą lektury samej decyzji, czy też poinformowania go o tych powodach na jego żądanie, bez uszczerbku dla uprawnienia właściwego sądu do zażądania podania tych powodów od właściwego organu, by umożliwić mu obronę swoich praw w najlepszych możliwych warunkach".[77] Sądy Unii Europejskiej mają zapewnić, by decyzja ta podjęta była na wystarczająco solidnej podstawie faktycznej[78]. Wyraźnie wskazano, że „nie można powołać się na tajność lub poufność [...] informacji lub dowodów, a przynajmniej nie przed sądami Unii Europejskiej[79]. Grupa Robocza uważa w związku z tym, że Rzecznik musi otrzymywać informacje i dowody na poparcie powodów realizacji środka, aby spełnić wymagania narzucone przez TSUE[80].

[77] Kadi II pkt 100.
78 Kadi II pkt 119.
79 Kadi II pkt 125.
[80] Kadi II pkt 122; chociaż zaangażowany organ nie musi podawać wszystkich informacji i dowodów będących przyczyną realizacji środka.

Na chwilę obecną nie jest jasne, jaki będzie zakres uprawnień dochodzeniowych Rzecznika. Zarówno projekt decyzji Komisji jak i załącznik III otrzymany od Departamentu Stanu nie są zbyt jednoznaczne w tej kwestii. Grupa Robocza uważa, że Rzecznik powinien uzyskać wystarczające informacje, aby móc stwierdzić, czy czynność przetwarzania danych przez służby bezpieczeństwa odbywa się zgodnie z prawem, a jeśli nie, aby upewnić się, że niezgodność takiego przypadku zostanie naprawiona. Ani pismo z Departamentu Stanu, ani projekt decyzji Komisji nie wskazują, czy Rzecznik będzie miał bezpośredni dostęp do danych dotyczących określonej osoby fizycznej i tym samym przeprowadzi samodzielne dochodzenie, czy też może wyłącznie polegać na sprawozdaniach od innych urzędników rządu USA.

3.5.3.8 Uprawnienia zaradcze

Memorandum dosyć niejasno określa w jaki sposób Rzecznik może zarządzić naprawienie niezgodności. Oprócz wątpliwości dotyczących uprawnień dochodzeniowych dodatkowo niejasne jest, w jakim zakresie sam Rzecznik będzie w stanie skutecznie zarządzić naprawienie niezgodności oraz jaki będzie tego rezultat. Czy oznacza to, że dane uzyskane w sposób niezgodny (tj. nielegalnie) nie będą mogły już być wykorzystane w jakiejkolwiek procedurze i powinny być usunięte?

Grupa Robocza zakłada także, że Tarcza Prywatności nie przewiduje odwołania lub przeglądu „decyzji" podejmowanej przez Rzecznika.

Wreszcie, jeżeli chodzi o komunikację Rzecznika ze skarżącym, po rozpatrzeniu skargi Rzecznik nie może ujawnić, czy nastąpiło niezgodne z prawem zachowanie wspólnoty wywiadowczej. Udzielona odpowiedź będzie zawsze taka sama i nieokreślona. W sprawie Kadi II TSUE orzekł, że właściwy organ (jako organ nadzorczy) ma obowiązek podać przyczyny obejmujące wszystkie okoliczności mimo że w artykule 296 TFUE nie wymaga się szczegółowej odpowiedzi.[81]

3.5.4. Wnioski podsumowujące

Kwestia istnienia skutecznych środków ochrony prawnej budzi nadal zaniepokojenie WP29. Po pierwsze projekt decyzji w sprawie odpowiedniej ochrony danych osobowych nie daje jednoznacznej odpowiedzi na pytanie, w jakich sytuacjach i na jakich warunkach wstępnych osoby fizyczne mogą wszcząć postępowanie w celu ustalenia ich praw.

WP29 z zadowoleniem przyjmuje i docenia wprowadzenie alternatywnego mechanizmu środków ochrony prawnej w formie Rzecznika, co stanowi wyjątkowy element rozwoju stosunków pomiędzy UE a państwem trzecim. Niezależnie od potrzeby wyjaśnienia terminu „osoby fizyczne z USA" zgodnie z postulatem powyżej, mechanizm ten tworzy nowy sposób realizacji środków ochrony prawnej za pośrednictwem rządu USA w celu zapewnienia, że wszelkie dane osobowe wnioskodawcy są przetwarzane zgodnie z prawem USA.

[81] Kadi II pkt 116.

Jednocześnie w ramach oceny mechanizmu Rzecznika w porównaniu do standardów mających zastosowanie do niezależnego trybunału w rozumieniu art. 47 Karty i wymogów, które TSUE oraz Europejski Trybunał Praw Człowieka ustanowiły w ramach orzecznictwa w sprawach o inwigilację, WP29 zwraca uwagę na poważne niedociągnięcia. Po pierwsze istnieją obawy co do tego, czy Rzecznika można uznać za (w pełni i formalnie) niezależnego, szczególnie z powodu względnej łatwości odwoływania z tego stanowiska z powodów politycznych. Po drugie, nadal istnieją wątpliwości co do uprawnień Rzecznika w zakresie sprawowania skutecznej i ciągłej kontroli. W oparciu o informacje podane w załączniku III WP29 nie może wysnuć wniosku, że Rzecznik będzie mieć zawsze bezpośredni dostęp do wszystkich informacji, plików i systemów IT wymaganych do przeprowadzenia własnej analizy, ani że może on faktycznie zmusić agencje wywiadu do zakończenia niezgodnego przetwarzania danych, z pewnością w przypadku braku porozumienia co do kwestii zgodności z prawem przetwarzania danych lub braku takiej zgodności. Wątpliwości WP29 rozwiać mogą dalsze wyjaśnienia dotyczące stanowiska Rzecznika i jego uprawnień.

3.6 Uwagi podsumowujące w sprawie gwarancji i ograniczeń dotyczące organów bezpieczeństwa narodowego USA

WP29 przede wszystkim pragnie wyrazić swoje uznanie dla Komisji i władz USA za poczynione przez nie wysiłki na rzecz zwiększenia przejrzystości skutków, jakie amerykańskie programy inwigilacji mogą mieć na dane przekazywane na podstawie Tarczy Prywatności lub innego mechanizmu przekazywania danych. Od ujawnienia informacji przez Snowdena w czerwcu 2013 r. podjęto istotne działania. WP29 zwraca jednak uwagę, że wciąż istnieją pewne obawy. Absolutne wymagane minimum stanowią dodatkowe wyjaśnienia i informacje dotyczące praw i obowiązków na podstawie Tarczy Prywatności.

Dwie podstawowe sprawy będące przedmiotem troski WP29 to fakt, że władze USA nie wyłączyły w całości gromadzenia danych prowadzonego na masową skalę i bez różnicowania, a uprawnienia i stanowisko Rzecznika nie zostały opisane wystarczająco szczegółowo. Dodatkowo krajowe organy ochrony danych, zamiast organów nadzoru agencji wywiadu, powinny mieć prawo do wszczęcia postępowania przed Rzecznikiem w imieniu osoby fizycznej. Dodatkowo pomimo iż WP29 docenia próby wyeliminowania obaw i wątpliwości zgłaszanych przez organy ochrony danych, z zadowoleniem przyjęłaby dodatkowe gwarancje zapewniające, że wszelkie ingerencje programów inwigilacji USA spełniają warunki konieczne dla społeczeństwa demokratycznego.

4. OCENA GWARANCJI TARCZY PRYWATNOŚCI DOTYCZĄCYCH EGZEKWOWANIA PRAWA

4.1 Wprowadzenie

W odniesieniu do publicznego dostępu do danych osobowych w celach egzekwowania prawa WP29 zwraca uwagę na fakt, że zasady prywatności w załączniku II do Tarczy Prywatności zawierają odstępstwo identyczne jak odstępstwo zawarte w zasadach prywatności programu „bezpieczna przystań". Ogólny charakter tego odstępstwa został wobec tego utrzymany, co

oznacza, że nowe zasady w ramach Tarczy Prywatności umożliwiają ingerencję w prawa podstawowe osób, których dane osobowe przekazywane są z UE do USA „opartą na wymaganiach bezpieczeństwa narodowego i interesu publicznego lub krajowych przepisach Stanów Zjednoczonych”.[82]

Jednym z głównych przedmiotów krytyki decyzji w odniesieniu do programu „bezpieczna przystań” w sprawie Schrems było natomiast to, że „nie zawiera żadnego stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do Stanów Zjednoczonych”.

WP29 w związku z tym z zadowoleniem przyjmuje starania władz amerykańskich na rzecz naświetlenia ram prawnych dotyczących ingerencji w dane osobowe przekazywane na podstawie Tarczy Bezpieczeństwa w celach egzekwowania prawa, także w zakresie mających zastosowanie ograniczeń i gwarancji. Jednocześnie WP29 podkreśla, że w ramach dostępu organów publicznych należy uwzględniać fakt, że jakakolwiek ingerencja w prawa podstawowe do życia prywatnego i ochrony danych musi w społeczeństwie demokratycznym posiadać uzasadnienie. WP29 w związku z tym przeanalizowała gwarancje w zakresie egzekwowania prawa na podstawie Tarczy Prywatności korzystając z ram podanych w sekcji. 1.2 niniejszej opinii.

4.2 Zastosowanie zasadniczych gwarancji europejskich do dostępu organów egzekwowania prawa do danych przechowywanych przez korporacje

4.2.1 Dostęp organów egzekwowania prawa do danych osobowych powinien być zgodny z prawem i oparty na jasnych, precyzyjnych i dostępnych regułach.

Załącznik VII do Tarczy Prywatności zawiera pismo Departamentu Sprawiedliwości USA „przedstawia krótki opis głównych narzędzi dochodzeniowych wykorzystywanych w celu pozyskania danych handlowych i innych informacji przechowywanych w rejestrach prowadzonych przez korporacje w Stanach Zjednoczonych w celach związanych ze ściganiem w sprawach karnych lub w celach leżących w interesie publicznym (na potrzeby organów administracji cywilnej lub regulacyjnych), uwzględniając ograniczenia dostępu przyjęte w aktach stanowiących podstawę prawną”.

Wszystkie procedury wymienione w załączniku VII wynikają bezpośrednio z Konstytucji USA (czwarta poprawka), z przepisów ustawowych i proceduralnych lub z wytycznych i polityk Departamentu Sprawiedliwości. Jednak w załączniku VII nie odniesiono się do poszczególnych ustaw, które ustanawiają takie procedury, a raczej skoncentrowano się na opisaniu w skrócie samych postępowań. W załączniku VII podano także, że „przedsiębiorstwa mogą również podważyć zasadność składanych przez agencje administracyjne wniosków o udostępnienie danych w oparciu o inne podstawy prawne, w zależności od sektora, w którym prowadzą działalność, oraz od rodzaju danych znajdujących się w ich posiadaniu”, wraz z podaniem szeregu przykładów niestanowiących katalogu

[82] Schrems, pkt 87

zamkniętego, takich jak amerykańskie ustawy o tajemnicy bankowej, ustawa o rzetelnej sprawozdawczości kredytowej i ustawa o prawie do prywatności w kwestiach finansowych.

WP29 zwraca uwagę na fakt, że ramy przepisów, postępowań i polityk są fragmentaryczne oraz że mająca zastosowanie wobec danego wniosku o dostęp podstawa prawna będzie zależała od rodzaju danych, których wniosek dotyczy, charakteru przedsiębiorstwa, charakteru postępowania (karne, administracyjne, związane z innym interesem publicznym) oraz charakteru podmiotu wnioskującego o dostęp.

Ponieważ wszystkie mające zastosowanie zasady ograniczające dostęp organów egzekwowania prawa do danych przekazywanych na podstawie Tarczy Prywatności oparte są na Konstytucji, przepisach ustawowych oraz przejrzystych politykach Departamentu Sprawiedliwości, WP29 przyjmuje założenie dostępności tych zasad. Mimo to jasność i precyzyjność tych zasad ocenić można tylko dla poszczególnych rodzajów postępowań i wniosków o dostęp. WP29 w związku z tym ubolewa, że w oparciu o dane przekazane w załączniku VII do Tarczy Prywatności oraz ustalenia projektu decyzji w chwili obecnej nie jest w stanie wykonać takiej oceny.

4.2.2 Należy wykazać konieczność i proporcjonalność w odniesieniu do realizowanych zgodnych z prawem celów

WP29 odpowiednio uwzględnia fakt, że wystąpienie o dostęp do danych w celach egzekwowania prawa może być uznane za realizację zgodnego z prawem celu. Na przykład art. 8 ust. 2 EKPC akceptuje ingerencję w prawo do ochrony życia prywatnego ze strony organu władzy „z uwagi na (...) bezpieczeństwo publiczne; (...) ochronę porządku i zapobieganie przestępstwom". Ingerencja taka jest jednak akceptowalna tylko w przypadkach gdy jest konieczna i proporcjonalna[83].

Zgodnie z ustalonym orzecznictwem TSUE zasada proporcjonalności wymaga, by środki ustawodawcze proponujące ingerencję w prawa do życia prywatnego i ochrony danych osobowych „były odpowiednie do realizacji uzasadnionych celów, *którym akty te służą*, i nie wykraczały poza to, co jest konieczne do ich osiągnięcia"[84] (nasze podkreślenie). Dlatego ocena konieczności i proporcjonalności zawsze odbywa się w odniesieniu do konkretnego środka przewidzianego przez przepisy.

Władze USA wskazują w załączniku VII, że federalni prokuratorzy oraz śledczy mogą uzyskać dostęp do dokumentów i innych zarejestrowanych informacji podmiotów za pośrednictwem „różnego rodzaju obowiązkowych pism sądowych, takich jak wezwania do stawienia się przed wielką ławą przysięgłych, wezwania administracyjne oraz nakazy przeszukania" i mogą pozyskiwać innego rodzaju informacje „na podstawie aktów stanowiących podstawę prawną na szczeblu federalnym do kontroli rozmów telefonicznych oraz instalowania urządzeń rejestrujących połączenia przychodzące na gruncie prawa

[83] Zob. dokument roboczy w sprawie zasadniczych gwarancji europejskich, s. 7-9. Ogólna ocena zasady konieczności i proporcjonalności zawarta jest w opinii nr 01/2014 WP29 w sprawie zastosowania zasady konieczności i proporcjonalności oraz ochrony danych w obszarze egzekwowania prawa, 27 lutego 2014 r.
[84] Digital Rights Ireland, pkt 46 i orzecznictwo cytowane tamże.

karnego”[85]. Dodatkowo agencje posiadające obowiązki cywilne i regulacyjne mogą wystawiać wezwania dotyczące „rejestrów związanych z prowadzoną działalnością, informacji przechowywanych w formie elektronicznej lub dostarczenia innych przedmiotów materialnych”[86] W załączniku VII dodatkowo wskazano, że te postępowania prawne są wykorzystywane zasadniczo do uzyskania informacji od „korporacji” w USA, niezależnie od tego, czy są one objęte certyfikacją na podstawie Tarczy Prywatności i „niezależnie od narodowości osoby, której dane dotyczą”. Innymi słowy wydaje się, że ochrona udzielana jest podmiotom, a nie osobom fizycznym.

Oprócz załącznika VII, projekt decyzji, który oparty jest na zasadach Tarczy Prywatności, zawiera ustalenia Komisji dotyczące istnienia w USA reguł ograniczających ingerencję w prawa podstawowe osób, których dane osobowe zostały przekazane z Unii do Stanów Zjednoczonych na podstawie Tarczy Prywatności.

Ustalenia projektu decyzji dotyczą w szczególności mających zastosowanie ograniczeń i gwarancji na podstawie czwartej poprawki do Konstytucji USA, zgodnie z którymi przeszukania i zajęcia ze strony organów egzekwowania prawa przede wszystkim wymagają nakazu wystawionego przez sąd i wskazującego prawdopodobną przyczynę[87]. Ustalenia dotyczą także faktu, że w wyjątkowych sytuacjach, gdy wymóg dotyczący nakazu nie obowiązuje, egzekwowanie prawa podlega zasadzie racjonalności.[88]

Niezależnie od tego ustalenia nie wskazują wyraźnie, w jaki sposób gwarancje stosowane będą wobec osób spoza USA. W jednym z motywów projektu decyzji wskazuje się, że „prawo zapisane w czwartej poprawce nie przysługuje osobom niebędącym obywatelami ani rezydentami USA”[89]. W tym samych akapitach projektu decyzji podano także, że osoby spoza USA „pośrednio korzystają z praw przysługujących przedsiębiorstwom amerykańskim przechowującym dane osobowe, które są odbiorcami wniosków organów egzekwowania prawa”. WP29 z żalem zauważa jednak, że w ustaleniach tych brak jest odesłania do źródła prawa, czy to przepisów ustawowych czy orzecznictwa.

Ogólnie rzecz biorąc WP29 pragnie zauważyć, że system narzędzi dochodzeniowych wykorzystywanych w celu pozyskania danych handlowych i innych informacji przechowywanych w rejestrach prowadzonych przez korporacje w Stanach Zjednoczonych w celach związanych ze ściganiem w sprawach karnych lub w celach leżących w interesie publicznym, z uwzględnieniem ograniczeń dostępu i gwarancji, stanowi kompleksowy zestaw różnych środków. W oparciu o dostępne informacje nie można ocenić całości funkcjonowania tego systemu. W celu uzyskania prawdziwej oceny konieczności i proporcjonalności środków dochodzeniowych organów egzekwowania prawa w związku z prawami podstawowymi do życia prywatnego i ochrony danych konieczne jest przeprowadzenie szczegółowych ocen poszczególnych przypadków.

[85] Załącznik VII, s. 2;
[86] Załącznik VII, s. 4;
[87] Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych, motyw 107
[88] Tarcza Prywatności, motyw 107
[89] Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych, motyw 108

4.2.3 Należy stworzyć mechanizm niezależnego nadzoru

WP29 zwraca uwagę na fakt, że większość postępowań opisanych w załączniku VII zakłada decyzję sądu zanim organy władz uzyskają dostęp do danych (np. nakaz sądowy w przypadku urządzeń rejestrujących wybierane numery oraz urządzeń śledzących, nakaz sądowy w przypadku inwigilacji na podstawie federalnych przepisów w sprawie podsłuchów, nakaz przeszukania - reguła 41). Wydaje się jednak, że nie wszystkie z nich wymagają apriorycznego angażowania sądu. Na przykład władze administracyjne i regulacyjne „mogą wystawiać wezwania do stawienia"[90]. W takim przypadku istnieje możliwość kontroli sądowej ex post racjonalności takiego wezwania, ponieważ odbiorca wezwania administracyjnego może sprzeciwić się wezwaniu do sądu"[91].

W oparciu o dostępne informacje WP29 odnotowuje, że w odniesieniu do dostępu organów egzekwowania prawa do danych przechowywanych w USA, istnieje stosunkowo dokładny mechanizm niezależnej kontroli.

4.2.4 Należy zagwarantować dostęp osób fizycznych do skutecznych środków prawnych:

Jak wspomniano powyżej „prawo zapisane w czwartej poprawce nie przysługuje osobom niebędącym obywatelami ani rezydentami USA"[92]. Oznacza to, że osoba spoza USA nie może sprzeciwić się nakazowi stawiennictwa lub przeszukania w sądzie powołując się na czwartą poprawkę. W projekcie decyzji w sprawie odpowiedniej ochrony danych osobowych wskazano, że osoby spoza USA pośrednio korzystają z praw przysługujących przedsiębiorstwom amerykańskim przechowującym dane osobowe, które są odbiorcami wniosków organów egzekwowania prawa. WP29 zwraca jednak uwagę na fakt, że nawet gdyby ochrona taka była skuteczna, nie oznacza to, że dla osób fizycznych dostępne są skuteczne środki prawne, ponieważ podmiotem prawa do skutecznego środka prawnego w tym scenariuszu jest raczej spółka otrzymująca wniosek o dostęp, a nie osoba, której dane dotyczą.

Załącznik VII nie zawiera dodatkowych informacji dotyczących potencjalnych środków prawnych wynikających z przepisów ustawowych, które są dostępne dla osób spoza USA, gdy organy publiczne lub spółki niezgodnie z prawem udzielają dostępu do ich danych lub uzyskują go.

WP29 z zadowoleniem przyjmuje fakt, że niedawno przyjęta ustawa o sądowych środkach odwoławczych[93] przewiduje prawo do korzystania z nich dla osób spoza USA. Prawa takie są jednak ograniczone do zdefiniowanych działań: prawo do uzyskania sprostowania i dostępu do danych, a także koszty zastępstwa procesowego w przypadku, gdy „wyznaczona agencja federalna lub jej część" odmawia aktualizacji danych lub dostępu do nich, a także prawo do uzyskania środków prawa cywilnego w przypadku ujawnień danych w sposób „celowy lub rozmyślny".

[90] Załącznik VII, s. 4;
[91] Załącznik VII, s. 4;
[92] Projekt decyzji w sprawie odpowiedniej ochrony danych osobowych, motyw 108
[93] Ustawa o sądowych środkach odwoławczych z 2015 r. H.R. 1428.

Dodatkowo orzecznictwo USA, o którym mowa w przypisach do poszczególnych motywów projektu decyzji, w szczególności sprawa miasto Ontario przeciwko Quon[94], Maryland przeciwko King[95] i Samson przeciwko Kalifornii[96] nie mają znaczenia dla oceny, czy osoby spoza USA mogą wytoczyć powództwo w celu zakwestionowania legalności ingerencji w ich prawo do prywatności[97]. Wszystkie przypadki dotyczą prawa do życia prywatnego osób z USA, i wszystkie z nich zawierają decyzje Sądu Najwyższego USA, który co do zasady ograniczył stosowanie czwartej poprawki.

Ogólnie rzecz biorąc WP29 docenia i z zadowoleniem przyjmuje przyjęcie ustawy o sądowych środkach odwoławczych, lecz jednocześnie w dalszym ciągu wyraża wątpliwość, czy dla poszczególnych osób, których dane dotyczą skuteczne środki ochrony prawnej są rzeczywiście dostępne.

4.3 Uwagi podsumowujące

WP29 z zadowoleniem i uznaniem przyjmuje starania władz amerykańskich na rzecz naświetlenia ram prawnych dotyczących ingerencji w dane osobowe przekazywane na podstawie Tarczy Bezpieczeństwa UE-USA w celach egzekwowania prawa, także w zakresie mających zastosowanie ograniczeń i gwarancji.

WP29 zwraca uwagę na fakt, że system narzędzi dochodzeniowych organów egzekwowania prawa, w tym w zakresie mających zastosowanie ograniczeń i gwarancji, jest zarówno rozległy jak i złożony, a informacje podane w Tarczy Prywatności mają charakter hasłowy. WP29 w związku z tym ubolewa, że w oparciu o te ograniczone informacje (tj. załącznik VII do Tarczy Prywatności oraz ustalenia projektu decyzji) w chwili obecnej nie jest w stanie wykonać kompleksowej oceny w zakresie dostępności, przewidywalności oraz konieczności i proporcjonalności mających zastosowanie zasad. Niezależnie od innych ustaleń WP29 dotyczących Tarczy Prywatności i zawartych w niniejszej opinii, ocena taka może być częścią corocznego przeglądu Tarczy Bezpieczeństwa.

W odniesieniu do dostępu organów egzekwowania prawa WP29 zwraca uwagę na fakt istnienia stosunkowo dokładnego mechanizmu niezależnej kontroli. Dodatkowo WP29 z zadowoleniem przyjmuje przyjęcie ustawy o sądowych środkach odwoławczych, która udziela prawa do korzystania z nich osobom spoza USA. WP29 wskazuje jednak, że prawa te mają ograniczony charakter. Oprócz ustalenia, że osoba spoza USA nie mogłaby sprzeciwić się nakazowi stawiennictwa lub przeszukania w sądzie powołując się na czwartą poprawkę,

[94] *Miasto Ontario, Cal. przeciwko Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland przeciwko King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson przeciwko Kalifornii*, 547 U.S. 843, 848 (2006).
[97] W sprawie *Ontario v. Quon* sąd orzekł, że miasto Ontario nie naruszyło praw swoich pracowników wynikających z czwartej poprawki, jako że dostęp miasta do treści prywatnych wiadomości pracowników był racjonalny, ponieważ motywowany był zgodnym z prawem i związanym z pracą celem, a jego zakres nie był nadmierny. W sprawie *Samson przeciwko Kalifornii* sąd uznał, że „czwarta poprawka nie uniemożliwia funkcjonariuszowi policji przeszukania bez wcześniejszych podejrzeń osoby zwolnionej warunkowo z odbywania kary pozbawienia wolności". W sprawie *Maryland przeciwko King* sąd uznał, że jeżeli funkcjonariusze dokonują aresztowania, które motywowane jest prawdopodobną przyczyną zatrzymania i umieszczenia w areszcie podejrzanego o poważne przestępstwo, pobranie i analiza DNA aresztanta z wacika przykładanego do policzka jest, podobnie jak pobieranie odcisków palców i wykonywanie fotografii, zgodnym z prawem policyjnym postępowaniem rejestracyjnym, które jest racjonalne na podstawie czwartej poprawki.

pozostają wątpliwości, czy skuteczne środki ochrony prawnej są faktycznie dostępne dla poszczególnych osób, których dane dotyczą w obszarze egzekwowania prawa.

5. WNIOSKI I ZALECENIA

WP29 po pierwsze z zadowoleniem przyjmuje fakt, że w ciągu pięciu miesięcy od unieważnienia programu „bezpieczna przystań" zaprezentowano projekt decyzji w sprawie odpowiedniej ochrony danych osobowych, zawierającej wiele ulepszeń w porównaniu do poprzedniego mechanizmu. WP29 szczególnie usatysfakcjonowana jest rosnącą przejrzystością związaną z wprowadzeniem dwóch wykazów Tarczy Prywatności znajdujących się na stronie internetowej Departamentu Handlu: jeden z nich zawiera rejestr podmiotów przestrzegających zasad Tarczy Prywatności, a drugi obejmuje rejestr podmiotów, które w przeszłości uczestniczyły w tym programie, lecz już tego nie czynią. WP29 z zadowoleniem przyjmuje także większą przejrzystość w odniesieniu do dostępu organów publicznych do danych przekazywanych na podstawie Tarczy Prywatności w celach dotyczących bezpieczeństwa narodowego lub egzekwowania prawa. WP29 jest bardzo usatysfakcjonowana tym, że wszystkie przypadki przekazywania danych do USA od teraz będą objęte tym samym stopniem ochrony: przepisy prawa nie faworyzują bowiem żadnego z mechanizmów.

5.1 Trzy istotne kwestie budzące obawy

Pozostają jednak istotne kwestie budzące obawy, którymi w opinii WP29 należy się zająć.

Pierwsza z nich dotyczy faktu, iż w projekcie decyzji w sprawie odpowiedniej ochrony danych osobowych, nie zobowiązuje się podmiotów do usuwania danych, gdy nie są już potrzebne. Jest to kluczowy element prawa UE w zakresie ochrony danych, zapewniający, że dane przechowywane są nie dłużej niż jest to konieczne do realizacji celu, do którego zostały zebrane. Po drugie, WP29 wnioskuje z załącznika VI, że władze USA nie wykluczają całkowicie dalszego zbierania niezróżnicowanych danych na masową skalę. WP29 konsekwentnie twierdzi, że takie gromadzenie danych jest nieuzasadnioną ingerencją w prawa podstawowe osób fizycznych. Trzeci problem dotyczy wprowadzenia instytucji Rzecznika. Chociaż WP29 z zadowoleniem przyjmuje ten bezprecedensowy krok tworzący nowy mechanizm w zakresie środków ochrony prawnej i nadzoru dla osób fizycznych, ma także wątpliwości, czy Rzecznik posiada wystarczające uprawnienia pozwalające mu na skuteczne działanie. Należy przynajmniej podać wyjaśnienia w kwestii uprawnień i stanowiska Rzecznika i wykazać w ten sposób, że jest on rzeczywiście niezależny i może zapewnić skuteczny środek odwoławczy w przypadku nieodpowiedniego przetwarzania danych.

5.2 Zalecane wyjaśnienia

Oprócz spraw wspomnianych powyżej, w treści niniejszej opinii WP29 zwróciła uwagę na różne kwestie, które wymagają dalszych wyjaśnień w kontekście decyzji w sprawie odpowiedniej ochrony danych osobowych. Przede wszystkim dotyczą one konieczności

zagwarantowania, że kluczowe koncepcje ochrony danych stosowane w Tarczy Prywatności są definiowane i stosowane w sposób konsekwentny. Obecnie tak się nie dzieje. Korzystne byłoby umieszczenie glosariusza terminów w części zawierającej najczęściej zadawane pytania w sprawie Tarczy Prywatności po uzgodnieniu dokładnego brzmienia ich definicji przez UE i USA. WP29 stwierdza także, że wtórne przekazywanie danych osobowych z UE nie zostało wystarczająco ujęte, przede wszystkim jeśli chodzi o jego zakres, zasadę celowości i gwarancje dotyczące przekazywania danych przedstawicielom. Jeżeli chodzi o dostęp do danych na podstawie Tarczy Bezpieczeństwa przez organy egzekwowania prawa, problem stanowi przewidywalność legislacyjna wynikająca z rozbudowanego i złożonego charakteru systemu egzekwowania prawa w USA zarówno na poziomie stanowym jak i federalnym, a także ograniczonej ilości informacji podanych w decyzji w sprawie odpowiedniej ochrony danych osobowych.

Decyzja dotycząca Tarczy Prywatności jest pierwszą decyzją w sprawie odpowiedniej ochrony danych osobowych od momentu uzgodnienia co do zasady tekstu GDPR. Wiele ulepszeń na szczeblu ochrony danych oferowanej osobom fizycznym nie znalazło odzwierciedlenia w zasadach Tarczy Prywatności. WP29 w związku z tym zaleca, by wkrótce po wejściu w życie GDPR odbył się przegląd przedmiotowej decyzji w sprawie odpowiedniej ochrony danych osobowych, a także podobnych decyzji wydanych w przypadku państw trzecich.

Ostatnie zalecenie WP29, któremu należy poświęcić tutaj szczególną uwagę jest wspólny przegląd. WP29 z zadowoleniem przyjmuje fakt, że decyzja w sprawie odpowiedniej ochrony danych osobowych będzie podlegać corocznym przeglądom, przy szerokim udziale organów ochrony danych i innych właściwych stron. WP29 z zadowoleniem przyjęłaby przyjęcie porozumienia w spawie elementów wspólnego przeglądu, w tym dotyczących przygotowania i prezentacji sprawozdania z przeglądu przez wszystkie uczestniczące w nim strony, z odpowiednim wyprzedzeniem przed przeprowadzeniem pierwszego takiego przeglądu.