



Zbiór Orzeczeń

OPINIA RZECZNIKA GENERALNEGO
HENRIKA SAUGMANDSGAARDA ØE
przedstawiona w dniu 19 grudnia 2019 r.¹

Sprawa C-311/18

Data Protection Commissioner
przeciwko
Facebook Ireland Limited,
Maximillian Schrems,
przy udziale:
The United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

[wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez High Court (wysoki trybunał, Irlandia)]

Odesłanie prejudycjalne – Ochrona osób fizycznych w zakresie przetwarzania danych osobowych – Rozporządzenie (UE) 2016/679 – Artykuł 2 ust. 2 – Zakres stosowania – Przekazywanie danych osobowych do Stanów Zjednoczonych Ameryki w celach komercyjnych – Przetwarzanie przekazanych danych przez organy publiczne Stanów Zjednoczonych Ameryki do celów bezpieczeństwa narodowego – Artykuł 45 – Ocena odpowiedniego charakteru stopnia ochrony zapewnianego w państwie trzecim – Artykuł 46 – Odpowiednie zabezpieczenia zapewniane przez administratora – Standardowe klauzule ochrony danych – Artykuł 58 ust. 2 – Uprawnienia krajowych organów nadzorczych – Decyzja 2010/87/UE – Ważność – Decyzja wykonawcza (UE) 2016/1250 – „Tarcza Prywatności UE–USA” – Ważność – Artykuły 7, 8 i 47 Karty praw podstawowych Unii Europejskiej

Spis treści

I. Wprowadzenie	3
II. Ramy prawne	5
A. Dyrektywa 95/46/WE.....	5
B. RODO	6
C. Decyzja 2010/87	11

¹ Język oryginału: francuski.

D. Decyzja w sprawie Tarczy Prywatności	15
III. Postępowanie główne, pytania prejudycjalne i postępowanie przed Trybunałem	16
IV. Analiza	25
A. Uwagi wstępne	25
B. W przedmiocie dopuszczalności odesłania prejudycjalnego	27
1. W przedmiocie stosowania dyrektywy 95/46 <i>ratione temporis</i>	27
2. W przedmiocie tymczasowego charakteru wątpliwości wyrażonych przez DPC	28
3. W przedmiocie wątpliwości dotyczących ustalenia okoliczności faktycznych	29
C. W przedmiocie możliwości zastosowania prawa Unii do przekazywania danych osobowych w celach komercyjnych do państwa trzeciego, w którym mogą one być przetwarzane do celów bezpieczeństwa narodowego (pytanie pierwsze)	29
D. W przedmiocie stopnia ochrony wymaganego w związku z przekazywaniem danych na podstawie standardowych klauzul umownych (pierwsza część pytania szóstego)	31
E. W przedmiocie ważności decyzji 2010/87 w świetle art. 7, 8 i 47 karty (pytania siódme, ósme i jedenaste)	33
1. W przedmiocie obowiązków ciążących na administratorach	34
2. W przedmiocie obowiązków spoczywających na organach nadzorczych	37
F. W przedmiocie braku potrzeby udzielania odpowiedzi na pozostałe pytania prejudycjalne i badania ważności decyzji w sprawie Tarczy Prywatności	40
1. W przedmiocie braku potrzeby udzielania odpowiedzi przez Trybunał z uwagi na przedmiot sporu w postępowaniu głównym	41
2. Względę przemawiające przeciwko badaniu przez Trybunał pozostałych pytań w świetle przedmiotu toczącego się przed DPC postępowania	42
G. Uwagi uzupełniające dotyczące skutków i ważności decyzji w sprawie Tarczy Prywatności	45
1. Wpływ decyzji w sprawie Tarczy Prywatności na rozpatrywanie przez organ nadzorczy skargi dotyczącej zgodności z prawem przekazywania danych w oparciu o zabezpieczenia umowne	45
2. W przedmiocie ważności decyzji w sprawie Tarczy Prywatności	46
a) Wyjaśnienia dotyczące zakresu badania ważności decyzji stwierdzającej odpowiedni stopień ochrony	48
1) W przedmiocie kryteriów porównawczych umożliwiających ocenę merytorycznej równowagi stopnia ochrony	48
2) W przedmiocie konieczności zapewnienia odpowiedniego stopnia ochrony na etapie tranzytu danych	53
3) W przedmiocie uwzględnienia poczynionych przez Komisję i sąd odsyłający ustaleń faktycznych dotyczących prawa Stanów Zjednoczonych	55

4) W przedmiocie znaczenia standardu „merytorycznej równowagi”	56
b) W przedmiocie ważności decyzji w sprawie Tarczy Prywatności w świetle prawa do poszanowania życia prywatnego i do ochrony danych osobowych.....	57
1) W przedmiocie istnienia ingerencji.....	58
2) Charakter ingerencji w świetle wymogu, aby były one „przewidziane ustawą”	59
3) Warunek dotyczący braku naruszenia istoty praw podstawowych	61
4) W przedmiocie warunku dotyczącego dążenia do prawnie uzasadnionego celu	64
5) W przedmiocie niezbędności i proporcjonalności ingerencji	65
c) Ważność decyzji w sprawie Tarczy Prywatności w świetle prawa do skutecznego środka prawnego.....	69
1) W przedmiocie skuteczności przewidzianych w prawie Stanów Zjednoczonych środków ochrony prawnej	70
2) W przedmiocie wpływu mechanizmu mediacji na stopień ochrony prawa do skutecznego środka ochrony prawnej	73
V. Wnioski	75

I. Wprowadzenie

1. W związku z brakiem wspólnych zabezpieczeń dotyczących ochrony danych osobowych w skali ogólnoświatowej, transgraniczne przepływy takich danych wiążą się z ryzykiem przerwania ciągłości poziomu ochrony zapewnianego w ramach Unii Europejskiej. W trosce o ułatwienie tych przepływów przy jednoczesnym ograniczeniu powyższego ryzyka, prawodawca Unii ustanowił trzy mechanizmy, zgodnie z którymi dane osobowe mogą być przekazywane z Unii do państwa trzeciego.

2. W pierwszej kolejności, takie przekazywanie danych może odbywać się na podstawie decyzji, w której Komisja Europejska stwierdzi, że dane państwo trzecie zapewnia „odpowiedni stopień ochrony” danych, które są do niego przekazywane². W drugiej kolejności, w przypadku braku takiej decyzji, przekazywanie danych jest dozwolone, jeżeli zostaną zapewnione „odpowiednie zabezpieczenia”³. Zabezpieczenia te mogą przybrać postać zawieranych między podmiotami przekazującymi i odbierającymi dane umów zawierających standardowe klauzule ochrony danych przyjęte przez Komisję. W trzeciej kolejności, w RODO ustanowione zostały pewne odstępstwa oparte w szczególności na zgodzie osoby, której dane dotyczą, umożliwiające przekazanie danych do państwa trzeciego w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony albo odpowiednich zabezpieczeń⁴.

2 Zobacz art. 45 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. 2016, L 119, s. 1, zwane dalej „RODO”).

3 Zobacz art. 46 RODO.

4 Zobacz art. 49 RODO.

3. Niniejszy wniosek o wydanie orzeczenia w trybie prejudycjalnym przedłożony przez High Court (wysoki trybunał, Irlandia) dotyczy drugiego z tych mechanizmów. Ściślej rzecz ujmując, wniosek ten dotyczy ważności decyzji 2010/87/UE⁵ – w której Komisja ustanowiła standardowe klauzule umowne dla pewnych kategorii przekazywania danych – w świetle art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą”).

4. Wniosek ten został złożony w ramach sporu, jaki zaistniał pomiędzy Data Protection Commissioner (komisarzem ds. ochrony danych, Irlandia, zwanym dalej „DPC”) a Facebook Ireland Ltd i Maximillianem Schremsem. Maximillian Schrems wniósł do DPC skargę dotyczącą przekazania jego danych osobowych przez spółkę Facebook Ireland do jej spółki dominującej, Facebook Inc. z siedzibą w Stanach Zjednoczonych Ameryki (zwanymi dalej „Stanami Zjednoczonymi”). DPC uznał, że wydanie rozstrzygnięcia w przedmiocie tej skargi jest uzależnione od tego, czy decyzja 2010/87 jest ważna. W tym kontekście zwrócił się on do sądu odsyłającego o skierowanie do Trybunału Sprawiedliwości pytania w tym względzie.

5. Pragnę wskazać na wstępie, że w mojej ocenie analiza pytań prejudycjalnych nie doprowadziła do ujawnienia żadnej okoliczności, która mogłaby mieć wpływ na ważność decyzji 2010/87.

6. Ponadto sąd odsyłający dał wyraz pewnym wątpliwościom dotyczącym zasadniczo odpowiedniego charakteru stopnia ochrony, jaki zapewniają Stany Zjednoczone, w związku ingerowaniem przez amerykańskie organy wywiadu w korzystanie z praw podstawowych przez osoby, których dane są przekazywane do tego państwa trzeciego. Wątpliwości te w sposób pośredni podważają oceny poczynione przez Komisję w tym przedmiocie, zawarte w decyzji wykonawczej (UE) 2016/1250⁶. Mimo że dla rozstrzygnięcia sporu w postępowaniu głównym nie jest konieczne, aby Trybunał rozstrzygnął tę kwestię (w związku z czym proponuję mu, aby tego nie czynił), tytułem uzupełnienia przedstawię powody, które każą mi wątpić w ważność tej decyzji.

7. Całość mojej analizy będzie nakierowana na poszukiwanie równowagi między koniecznością wykazania „rozsądnego stopnia pragmatyzmu, w celu umożliwienia interakcji z resztą świata”⁷ z jednej strony, i, z drugiej strony, koniecznością afirmacji podstawowych wartości uznanych w porządkach prawnych Unii i jej państw członkowskich, w szczególności w karcie.

5 Decyzja Komisji z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady (Dz.U. 2010, L 39, s. 5), zmieniona decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r. (Dz.U. 2016, L 344, s. 100) (zwana dalej „decyzją 2010/87”).

6 Decyzja Komisji z dnia 12 lipca 2016 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, przyjęta na mocy [dyrektywy 95/46] (Dz.U. 2016, L 207, s. 1) (zwana dalej „decyzją w sprawie Tarczy Prywatności”).

7 Zobacz przemówienie byłego Europejskiego Inspektora Ochrony Danych (CEPD) P. Hustinx, *Le droit de l'Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données*, s. 49, dostępny na stronie internetowej https://edps.europa.eu/sites/edp/files/publication/1409-15_article_eui_fr.pdf.

II. Ramy prawne

A. Dyrektywa 95/46/WE

8. Artykuł 3 ust. 2 dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych⁸ stanowił:

„Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:

- w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności państwa w obszarach prawa karnego,

[...]”.

9. Artykuł 13 ust. 1 tej dyrektywy miał następujące brzmienie:

„Państwo członkowskie może przyjąć środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków, przewidzianego w art. 6 ust. 1, art. 10, art. 11 ust. 1, art. 12 oraz 21, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia:

- a) bezpieczeństwa narodowego;
- b) obronności;
- c) bezpieczeństwa publicznego;
- d) działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacji;
- e) ważnego interesu ekonomicznego lub finansowego państwa członkowskiego lub [Unii], łącznie z kwestiami pieniężnymi, budżetowymi i podatkowymi;
- f) funkcji kontrolnych, inspekcyjnych i regulacyjnych związanych, nawet sporadycznie, z wykonywaniem władzy publicznej w przypadkach wymienionych w lit. c)–e);
- g) ochrony osoby, której dane dotyczą oraz praw i wolności innych osób”.

10. Artykuł 25 tej dyrektywy miał następujące brzmienie:

„1. Państwa członkowskie zapewniają, aby przekazywanie do państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu mogło nastąpić tylko wówczas gdy, niezależnie od zgodności z krajowymi przepisami przyjętymi na podstawie innych przepisów niniejszej dyrektywy, dane państwo trzecie zapewni odpowiedni stopień ochrony.

⁸ Dyrektywa Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. (Dz.U. 1995, L 281, s. 31 – wyd. spec. w jęz. polskim, rozdz. 13, t. 15, s. 355) zmieniona rozporządzeniem (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. (Dz.U. 2003, L 284, s. 1 – wyd. spec. w jęz. polskim, rozdz. 1, t. 4, s. 447) (zwana dalej „dyrektywą 95/46”).

2. Odpowiedni stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji; szczególną uwagę zwracać się będzie na charakter danych, cel i czas trwania proponowanych operacji przetwarzania danych, kraj pochodzenia i kraj ostatecznego przeznaczenia, przepisy prawa, zarówno ogólne jak i branżowe, obowiązujące w państwie trzecim oraz przepisy zawodowe i środki bezpieczeństwa stosowane w tym państwie.

[...]

6. Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia prawidłowy stopień ochrony w znaczeniu ust. 2 niniejszego artykułu, co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, jakie państwo to przyjęło, szczególnie po zakończeniu negocjacji określonych w ust. 5, w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych.

Państwa członkowskie podejmują środki niezbędne w celu wykonania decyzji Komisji”.

11. Artykuł 26 ust. 2 i 4 tej dyrektywy stanowił:

„2. Bez uszczerbku dla ust. 1, państwo członkowskie może zezwolić na przekazanie lub przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2, jeżeli administrator danych zaleci odpowiednie zabezpieczenia odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw; takie środki zabezpieczające mogą w szczególności wynikać z odpowiednich klauzul umownych.

[...]

4. Jeżeli Komisja postanowi [...], że określone klauzule umowne zapewniają odpowiednie środki zabezpieczające wymagane w ust. 2, państwa członkowskie podejmą konieczne środki w celu zastosowania się do decyzji Komisji”.

12. Artykuł 28 ust. 3 dyrektywy 95/46 brzmiał następująco:

„Każdy organ jest w szczególności wyposażony w:

[...]

– skuteczne uprawnienia interwencyjne, jak np. prawo do wyrażania opinii przed przystąpieniem do operacji przetwarzania danych zgodnie z art. 20, oraz zapewnienia odpowiedniej publikacji swoich opinii, zarządzania blokady, usunięcia lub zniszczenia danych, nakładania czasowego lub ostatecznego zakazu przetwarzania danych, ostrzegania lub upominania administratora danych, lub też prawo kierowania sprawy do parlamentów narodowych lub innych instytucji politycznych,

[...]”.

B. RODO

13. Artykuł 94 ust. 1 RODO uchylił dyrektywę 95/46 ze skutkiem od dnia 25 maja 2018 r., począwszy od którego to dnia rozporządzenie to ma zastosowanie, zgodnie z jego art. 99 ust. 2.

14. Artykuł 2 ust. 2 tego rozporządzenia stanowi:

„Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:

- a) w ramach działalności nieobjętej zakresem prawa Unii;
- b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

[...]

- d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom”.

15. Artykuł 4 pkt 2 tego rozporządzenia definiuje „przetwarzanie” jako „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie”.

16. Artykuł 23 RODO stanowi:

„1. Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym:

- a) bezpieczeństwu narodowemu;
- b) obronie;
- c) bezpieczeństwu publicznemu;
- d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;
- e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego [...];

[...]

2. W szczególności akt prawny, o którym mowa w ust. 1, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:

- a) celach przetwarzania lub kategorii przetwarzania;
- b) kategoriach danych osobowych;

- c) zakresie wprowadzonych ograniczeń;
- d) zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu;
- e) określeniu administratora lub kategorii administratorów;
- f) okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania;
- g) ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz
- h) prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia”.

17. Artykuł 44 tego rozporządzenia, zatytułowany „Ogólna zasada przekazywania”, stanowi:

„Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy – z zastrzeżeniem innych przepisów niniejszego rozporządzenia – administrator i podmiot przetwarzający spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu”.

18. Zgodnie z art. 45 tego rozporządzenia zatytułowanym „Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony”:

„1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

2. Oceniając, czy stopień ochrony jest odpowiedni, Komisja uwzględnia w szczególności następujące elementy:

- a) praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo, a także istnienie skutecznych i egzekwowalnych praw osób, których dane dotyczą, oraz prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia;
- b) istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub w stosunku do organizacji międzynarodowej, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z organami nadzorczymi państw członkowskich; oraz

c) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych.

3. Po dokonaniu oceny, czy stopień ochrony jest odpowiedni, Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu. W akcie wykonawczym przewiduje się mechanizm okresowego przeglądu – przynajmniej raz na cztery lata – podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej. [...]

4. Komisja na bieżąco monitoruje zmiany w państwach trzecich i organizacjach międzynarodowych mogące wpłynąć na obowiązywanie decyzji przyjętych na mocy ust. 3 niniejszego artykułu oraz decyzji przyjętych na podstawie art. 25 ust. 6 [dyrektywy 95/46].

5. Jeżeli dostępne informacje na to wskazują, w szczególności po przeglądzie, o którym mowa w ust. 3 niniejszego artykułu, Komisja przyjmuje decyzję stwierdzającą, że państwo trzecie – lub terytorium lub jeden lub więcej określonych sektorów w tym państwie trzecim – lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony w rozumieniu ust. 2 niniejszego artykułu, i w niezbędnym zakresie uchyla, zmienia lub zawiesza decyzję, o której mowa w ust. 3 niniejszego artykułu, w drodze aktów wykonawczych bez mocy wstecznej. [...]

6. Komisja podejmuje konsultacje z państwem trzecim lub organizacją międzynarodową w celu zaradzenia sytuacji będącej przyczyną decyzji przyjętej na mocy ust. 5.

[...]

9. Decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 [dyrektywy 95/46] pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylecia decyzją Komisji przyjętą zgodnie z ust. 3 lub 5 niniejszego artykułu”.

19. Artykuł 46 tego rozporządzenia, zatytułowany „Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń”, ma następujące brzmienie:

„1. W razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej.

2. Odpowiednie zabezpieczenia, o których mowa w ust. 1, można zapewnić – bez konieczności uzyskania specjalnego zezwolenia ze strony organu nadzorczego – za pomocą:

[...]

c) standardowych klauzul ochrony danych przyjętych przez Komisję zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2;

[...]

5. Zezwolenia wydane przez państwo członkowskie lub organ nadzorczy na podstawie art. 26 ust. 2 [dyrektywy 95/46] zachowują ważność do czasu ich zmiany, zastąpienia lub uchylecia w razie potrzeby przez ten organ. Decyzje przyjęte przez Komisję na mocy art. 26 ust. 4 [dyrektywy 95/46] pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylecia w razie potrzeby decyzją Komisji przyjętą zgodnie z ust. 2 niniejszego artykułu”.

20. Zgodnie z art. 58 ust. 2, 4 i 5 RODO:

„2. Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia naprawcze:

- a) wydawanie ostrzeżeń administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania;
- b) udzielanie upomnień administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania;
- c) nakazanie administratorowi lub podmiotowi przetwarzającemu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
- d) nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu;
- e) nakazanie administratorowi zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych;
- f) wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania;

[...]

- i) zastosowanie, oprócz lub zamiast środków, o których mowa w niniejszym ustępie, administracyjnej kary pieniężnej na mocy art. 83, zależnie od okoliczności konkretnej sprawy;
- j) zakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

[...]

4. Wykonywanie uprawnień powierzonych organowi nadzorczemu na mocy niniejszego artykułu podlega odpowiednim zabezpieczeniom – w tym prawu do skutecznego środka ochrony prawnej przed sądem i rzetelnego procesu, określonym w prawie Unii i prawie państwa członkowskiego zgodnie z kartą.

5. Każde państwo członkowskie przewiduje w swoich przepisach, że jego organ nadzorczy jest uprawniony do wniesienia do organów wymiaru sprawiedliwości sprawy dotyczącej naruszenia niniejszego rozporządzenia oraz w stosownych przypadkach do wszczęcia lub do uczestniczenia w inny sposób w postępowaniu sądowym w celu wyegzekwowania stosowania przepisów niniejszego rozporządzenia”.

C. Decyzja 2010/87

21. W oparciu o art. 26 ust. 4 dyrektywy 95/46 Komisja przyjęła trzy decyzje (zwane dalej „decyzjami w sprawie standardowych klauzul umownych”)⁹, w których stwierdziła, że sformułowane w nich standardowe klauzule umowne zapewniają odpowiednie gwarancje ochrony prywatności oraz podstawowych praw i wolności osób fizycznych oraz wykonywania odpowiednich praw.

22. Jedną z tych decyzji jest decyzja 2010/87, której art. 1 stanowi, że „[s]tandardowe klauzule umowne określone w załączniku uważa się za zapewniające odpowiednie gwarancje ochrony prywatności oraz podstawowych praw i wolności osób fizycznych oraz wykonywania odpowiednich praw zgodnie wymogami art. 26 ust. 2 [dyrektywy 95/46]”.

23. Zgodnie z art. 3 tej decyzji:

„Do celów niniejszej decyzji stosuje się poniższe definicje:

[...]

- c) »podmiot przekazujący dane« oznacza administratora danych, który przekazuje dane osobowe;
- d) »podmiot odbierający dane« oznacza administratora danych prowadzącego działalność gospodarczą w państwie trzecim, który wyraża zgodę na otrzymywanie od podmiotu przekazującego danych osobowych w celu ich przetwarzania w imieniu podmiotu przekazującego po przekazaniu zgodnie z instrukcjami tego ostatniego i warunkami określonymi w niniejszej decyzji i który nie podlega systemowi państwa trzeciego zapewniającemu odpowiednią ochronę w rozumieniu art. 25 ust. 1 dyrektywy [95/46];

[...]

- f) »właściwe prawo o ochronie danych« oznacza prawodawstwo chroniące podstawowe prawa i wolności osób fizycznych, a w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych, właściwe dla administratora danych w państwie członkowskim, w którym podmiot przekazujący dane prowadzi działalność gospodarczą;

[...]”.

24. W pierwotnej wersji art. 4 ust. 1 tej decyzji miał następujące brzmienie:

„Bez uszczerbku dla swoich kompetencji do podejmowania działań w celu zapewnienia zgodności z przepisami prawa krajowego przyjętego na mocy rozdziałów II, III, V i VI [dyrektywy 95/46], właściwe organy w państwach członkowskich mogą wykonywać przysługujące im obecnie uprawnienia do zakazania lub zawieszenia przekazywania danych do państw trzecich w celu ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych, w przypadkach, w których:

- a) ustalono, że prawo, któremu podlega podmiot odbierający dane lub podwykonawca przetwarzania, nakłada na niego wymagania dotyczące odstępowania od stosowania zasad ochrony danych, które wykraczają poza ograniczenia konieczne w demokratycznym społeczeństwie w rozumieniu

⁹ Decyzja Komisji 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy [95/46] (Dz.U. 2001, L 181, s. 19 – wyd. spec. w jęz. polskim, rozdz. 13, t. 26, s. 347); decyzja Komisji 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję [2001/497] w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich (Dz.U. 2004, L 385, s. 74) oraz decyzja 2010/87.

w art. 13 [dyrektywy 95/46], jeżeli wymagania te mogą mieć istotne negatywne skutki dla gwarancji ustanowionych we właściwym prawie o ochronie danych i w standardowych klauzulach umownych;

- b) właściwy organ ustalił, że podmiot odbierający dane lub podwykonawca przetwarzania naruszył standardowe klauzule umowne określone w załączniku; lub;
- c) istnieje istotne prawdopodobieństwo, że standardowe klauzule umowne zawarte w załączniku nie są lub nie będą przestrzegane, a kontynuowanie przekazywania danych może stworzyć realne zagrożenie wyrządzenia poważnej szkody osobom, których dane dotyczą”.

25. W aktualnym brzmieniu wynikającym ze zmiany decyzji 2010/87 dokonanej decyzją wykonawczą (UE) 2016/2297¹⁰, art. 4 decyzji 2010/87 stanowi, że „[w] przypadku gdy właściwe organy w państwach członkowskich wykonują swoje uprawnienia na podstawie art. 28 ust. 3 [dyrektywy 95/46], co prowadzi do zawieszenia lub ostatecznego zakazu przepływu danych do państw trzecich w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, dane państwo członkowskie bezzwłocznie informuje o tym Komisję, która przekazuje tę informację pozostałym państwom członkowskim”.

26. Załącznik do decyzji 2010/87 zawiera szereg standardowych klauzul umownych. W szczególności klauzula 3 zawarta w tym załączniku, nosząca tytuł „Klauzula na rzecz osoby trzeciej”, stanowi:

„1. Osoba, której dotyczą dane, może żądać od podmiotu przekazującego dane wykonania niniejszej klauzuli, klauzuli 4 lit. b)–i), klauzuli 5 lit. a)–e) oraz lit. g)–j), klauzuli 6 pkt 1 i 2, klauzuli 7, klauzuli 8 pkt 2 i klauzuli [klauzul] 9–12, jako osoba trzecia, na rzecz której zawarto umowę.

2. Osoba, której dotyczą dane, może żądać od podmiotu odbierającego dane wykonania niniejszej klauzuli, klauzuli 5 lit. a)–e) oraz lit. g), klauzuli 6, klauzuli 7, klauzuli 8 pkt 2 i klauzul 9–12 w przypadkach, w których podmiot przekazujący dane przestał istnieć faktycznie lub formalnie. Jeżeli jednak na podstawie umowy lub z mocy prawa podmiot będący jego następcą przejął wszystkie zobowiązania prawne podmiotu przekazującego dane, skutkiem czego przyjął na siebie jego prawa i obowiązki, osoba, której dane dotyczą, może żądać wykonania wymienionych klauzul od tego następcy.

[...]”.

27. Klauzula 4 sformułowana w tym załączniku, zatytułowana „Obowiązki podmiotu przekazującego dane”, ma następujące brzmienie:

„Podmiot przekazujący dane zgadza się na poniższe warunki i gwarantuje, że:

- a) przetwarzanie danych, włącznie z samym ich przekazywaniem, odbywało się i będzie się nadal odbywało zgodnie z odpowiednimi przepisami właściwego prawa o ochronie danych (i w stosownych przypadkach było przedmiotem powiadomienia odpowiednich władz państwa członkowskiego, w którym podmiot przekazujący dane prowadzi działalność gospodarczą) oraz bez naruszenia odpowiednich przepisów tego państwa;
- b) nakazał i będzie nakazywał podmiotowi odbierającemu dane podczas całego okresu świadczenia usług przetwarzania danych osobowych, przetwarzanie przekazywanych danych osobowych wyłącznie w imieniu podmiotu przekazującego dane oraz zgodnie z właściwym prawem o ochronie danych i z niniejszymi klauzulami;

10 Decyzja Komisji z dnia 16 grudnia 2016 r. zmieniająca decyzje [2001/497] i [2010/87] w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych państwom trzecim oraz podmiotom przetwarzającym dane mającym siedzibę w takich państwach, na mocy dyrektywy [95/46] (Dz.U. 2016, L 344, s. 100).

- c) podmiot odbierający dane zapewni wystarczające gwarancje w odniesieniu do technicznych i organizacyjnych środków bezpieczeństwa wyszczególnionych w dodatku 2 do niniejszej umowy;
- d) biorąc pod uwagę ocenę wymogów właściwego prawa o ochronie danych osobowych, środki bezpieczeństwa są odpowiednie do ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, przypadkową utratą, zmianą, nieupoważnionym ujawnieniem lub dostępem, w szczególności jeżeli przetwarzanie obejmuje przekazywanie danych za pomocą sieci, oraz przed innymi niezgodnymi z prawem formami przetwarzania, a także że środki te zapewniają poziom bezpieczeństwa odpowiedni do ryzyka, jakie stanowi przetwarzanie i charakter danych podlegających ochronie, uwzględniając stan wiedzy w tej dziedzinie i koszty ich wdrożenia;
- e) zapewni zgodność ze środkami bezpieczeństwa;
- f) jeżeli przekazanie obejmuje szczególne kategorie danych, osoba, której dane dotyczą, została poinformowana lub będzie poinformowana przed przekazaniem lub jak najszybciej po przekazaniu o tym, że jej dane mogą być przekazane do państwa trzeciego, które nie zapewnia odpowiedniej ochrony w rozumieniu [dyrektywy 95/46];
- g) prześle wszelkie zawiadomienia otrzymane od podmiotu odbierającego dane lub podwykonawcy przetwarzania na mocy klauzuli 5 lit. b) i klauzuli 8 pkt 3 do organu nadzorczego ds. ochrony danych, jeżeli podmiot przekazujący dane zdecyduje się kontynuować przekazywanie danych lub znieść zawieszenie;
- h) na żądanie udostępni osobie, której dotyczą dane, kopię niniejszych klauzul, z wyjątkiem dodatku 2, oraz skrócony opis środków bezpieczeństwa, a także kopię każdej umowy dotyczącej usług podwykonawstwa przetwarzania danych, która musi być zawarta zgodnie z niniejszymi klauzulami; jednakże w przypadku gdy klauzule lub umowa zawierają informacje handlowe, informacje te można usunąć;
- i) w przypadku podwykonawstwa przetwarzania danych działalność związana z przetwarzaniem prowadzona jest zgodnie z klauzulą 11 przez podwykonawcę przetwarzającego co najmniej ten sam poziom ochrony danych osobowych i praw osoby, której dane dotyczą, co podmiot odbierający dane zgodnie z niniejszymi klauzulami; oraz;
- j) zapewni zgodność z klauzulą 4 lit. a)–i)”.

28. Klauzula 5 zawarta w tym załączniku, zatytułowana „Obowiązki podmiotu odbierającego dane” ma następujące brzmienie:

„Podmiot odbierający dane zgadza się na poniższe warunki i gwarantuje, że:

- a) będzie przetwarzał dane osobowe wyłącznie w imieniu podmiotu przekazującego dane i zgodnie z jego instrukcjami oraz niniejszymi klauzulami; jeżeli z jakichkolwiek powodów nie może zapewnić takiej zgodności, zgadza się na natychmiastowe poinformowanie podmiotu przekazującego dane o niemożności spełnienia tego warunku, a podmiot przekazujący dane jest w takim przypadku uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy;
- b) nie ma powodu, by sądzić, że prawodawstwo mające do niego zastosowanie uniemożliwia mu wypełnianie instrukcji otrzymanych od podmiotu przekazującego dane i jego obowiązków wynikających z umowy oraz że w przypadku zmiany prawodawstwa, która może mieć istotne negatywne skutki dla gwarancji i obowiązków określonych w niniejszych klauzulach, zawiadomi o tym jak najszybciej podmiot przekazujący dane, który w takim przypadku jest uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy;

- c) wdrożył techniczne i organizacyjne środki bezpieczeństwa wyszczególnione w dodatku 2 przed przetwarzaniem przekazanych danych osobowych;
- d) niezwłocznie powiadomi podmiot przekazujący dane o:
 - (i) jakichkolwiek prawnie wiążących wnioskach o ujawnienie danych osobowych ze strony organów ścigania, chyba że powiadomienie o takim wniosku jest zakazane, na przykład na mocy prawa karnego w celu zachowania poufności postępowań prowadzonych przez organy ścigania;
 - (ii) jakimkolwiek przypadkowym lub nieupoważnionym dostępie; oraz
 - (iii) jakimkolwiek żądaniu otrzymanym bezpośrednio od osób, których dotyczą dane, bez udzielenia odpowiedzi na to żądanie, chyba że został on w inny sposób upoważniony do takiego postępowania;
- e) niezwłocznie i we właściwy sposób zajmie się wszystkimi zapytaniami ze strony podmiotu przekazującego dane, dotyczącymi przetwarzania przez siebie danych osobowych będących przedmiotem przekazania, oraz zastosuje się do zaleceń organów nadzorczych w odniesieniu do przetwarzania przekazywanych danych;
- f) na żądanie podmiotu przekazującego dane przedstawi swoje urządzenia do przetwarzania danych w celu kontroli działalności związanej z przetwarzaniem danych objętej niniejszymi klauzulami, przeprowadzanej przez podmiot przekazujący dane lub organ kontrolny złożony z niezależnych członków i posiadający wymagane kwalifikacje zawodowe, związany obowiązkiem zachowania poufności, wybrany przez podmiot przekazujący dane, w stosownych przypadkach w porozumieniu z organem nadzorczym;

[...]”.

29. Zgodnie z przepisem 1, do którego odsyła tytuł klauzuli 5 załącznika do decyzji 2010/87:

„Obowiązujące wymogi przepisów krajowych mające zastosowanie do podmiotu odbierającego dane, które nie wykraczają poza to, co konieczne w demokratycznym społeczeństwie na podstawie jednego z interesów wymienionych w art. 13 ust. 1 dyrektywy [95/46] (tj. jeżeli stanowią środek konieczny do zabezpieczenia: bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, zapobiegania przestępstwom lub czynom stanowiącym naruszenie zasad etyki w zawodach regulowanych i ich dochodzenia, wykrywania i ścigania, ważnego interesu ekonomicznego lub finansowego państwa lub ochrony osoby, której dane dotyczą, lub praw i wolności innych osób), nie są sprzeczne ze standardowymi klauzulami umownymi. Niektóre przykłady wspomnianych bezwzględnie obowiązujących wymogów niewykraczających poza to, co konieczne w demokratycznym społeczeństwie, to m.in. sankcje uznane na szczeblu międzynarodowym, wymagania związane ze sprawozdawczością podatkową lub w zakresie przeciwdziałania praniu pieniędzy”.

30. Klauzula 6 zawarta w tym załączniku, zatytułowana „Odpowiedzialność”, ma następujące brzmienie:

„1. Strony uzgadniają, że każda osoba, której dotyczą dane, która poniosła szkodę w wyniku jakiegokolwiek naruszenia obowiązków, o których mowa w klauzuli 3 lub 11, przez którąkolwiek ze stron lub podwykonawcę przetwarzania, jest uprawniona do uzyskania odszkodowania za poniesioną szkodę od podmiotu przekazującego dane.

2. Jeżeli osoba, której dane dotyczą, nie jest w stanie wystąpić przeciw podmiotowi przekazującemu dane z roszczeniem o odszkodowanie zgodnie z pkt 1, wynikającym z naruszenia przez podmiot odbierający dane lub jego podwykonawcę przetwarzania któregośkolwiek z ich obowiązków, o których mowa w klauzuli 3 lub klauzuli 11, ponieważ podmiot przekazujący dane przestał istnieć faktycznie lub formalnie lub stał się niewypłacalny, podmiot odbierający dane zgadza się na wystąpienie przez osobę, której dane dotyczą, z roszczeniem wobec podmiotu odbierającego dane, tak jakby był on podmiotem przekazującym dane; jeżeli jednak jakkolwiek podmiot będący jego następcą przejął na podstawie umowy lub z mocy prawa wszystkie zobowiązania prawne podmiotu przekazującego dane, osoba, której dane dotyczą, może egzekwować swoje prawa wobec tego następcy.

[...]”.

31. Klauzula 7 zawarta w omawianym załączniku, zatytułowana „Mediacja i sąd właściwy”, stanowi:

„1. Podmiot odbierający dane zgadza się na to, że jeżeli osoba, której dane dotyczą, powołuje się wobec niego na prawa osoby trzeciej, na rzecz której zawarto umowę lub występuje o odszkodowanie za szkody na podstawie niniejszych klauzul, podmiot odbierający dane przyjmie decyzję osoby, której dane dotyczą, o:

- a) przekazaniu sporu do mediacji prowadzonej przez niezależną osobę lub, w stosownych przypadkach, organ nadzorczy;
- b) przekazaniu sporu do sądów w państwie członkowskim, w którym prowadzi działalność gospodarczą podmiot przekazujący dane.

2. Strony uzgadniają, że wybór osoby, której dane dotyczą, nie będzie naruszał jej materialnych lub proceduralnych praw do środków ochrony prawnej zgodnie z odrębnymi przepisami prawa krajowego lub międzynarodowego”.

32. Zawarta w tym samym załączniku klauzula 9, zatytułowana „Prawo właściwe” przewiduje, że standardowe klauzule umowne podlegają prawu państwa członkowskiego, w którym prowadzi działalność podmiot przekazujący dane.

D. Decyzja w sprawie Tarczy Prywatności

33. Artykuł 25 ust. 6 dyrektywy 95/46 posłużył za podstawę do przyjęcia przez Komisję dwóch kolejnych decyzji, w których stwierdziła ona, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych mającym siedziby w tym kraju przedsiębiorstwom, które w ramach procedury samocertyfikacji złożyły oświadczenia o zobowiązaniu się do przestrzegania zasad wyrażonych w tych decyzjach.

34. W pierwszej kolejności Komisja przyjęła decyzję 2000/520/WE w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach „bezpiecznej przystani” oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu [Stanów Zjednoczonych]¹¹. W wyroku z dnia 6 października 2015 r., Schrems¹² Trybunał stwierdził nieważność tej decyzji.

35. W drugiej kolejności, w następstwie tego wyroku, Komisja przyjęła decyzję w sprawie „Tarczy Prywatności”.

11 Decyzja z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy [95/46] (Dz.U. 2000, L 215, s. 7 – wyd. spec. w jęz. polskim, rozdz. 16, t. 1, s. 119, zwana dalej „decyzją w sprawie bezpiecznej przystani”).

12 Wyrok w sprawie C-362/14 (EU:C:2015:650) (zwany dalej „wyrokiem Schrems”).

36. Artykuł 1 tej decyzji stanowi:

„1. Do celów art. 25 ust. 2 [dyrektywy 95/46] Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do podmiotów w Stanach Zjednoczonych w ramach Tarczy Prywatności UE–USA.

2. Na Tarczę Prywatności UE–USA składają się zasady wydane przez Departament Handlu Stanów Zjednoczonych w dniu 7 lipca 2016 r., jak wskazano w załączniku II, oraz oficjalne oświadczenia i zobowiązania zawarte w dokumentach przedstawionych w załącznikach I, III–VII.

3. Do celów ust. 1 dane osobowe są przekazywane w ramach Tarczy Prywatności UE–USA, w przypadku gdy przekazuje się je z Unii do podmiotów w Stanach Zjednoczonych, które figuruje w „wykazie podmiotów uczestniczących w programie Tarczy Prywatności” prowadzonym i udostępnianym publicznie przez Departament Handlu Stanów Zjednoczonych zgodnie z sekcjami I i III zasad przedstawionych w załączniku II”.

37. Załącznik III A do tej decyzji, zatytułowany „Urząd Rzecznika ds. Tarczy Prywatności UE–USA w odniesieniu do rozpoznania radioelektronicznego”, dołączony do pisma ówczesnego Secretary of State (Sekretarza Stanu, Stany Zjednoczone) Johna Kerry’ego, z dnia 7 lipca 2016 r., zawiera memorandum opisujące nową procedurę mediacji przeprowadzaną przed „starszym rzecznikiem ds. międzynarodowej dyplomacji w dziedzinie technologii informacyjnej” (zwanym dalej „rzecznikiem”) wyznaczonym przez Sekretarza Stanu.

38. Zgodnie z powyższym memorandum procedura ta została wdrożona „aby ułatwić rozpatrywanie wniosków dotyczących dostępu ze względów bezpieczeństwa narodowego do danych przekazywanych Stanom Zjednoczonym przez [Unię] zgodnie z Tarczą Prywatności, standardowymi klauzulami umownymi, wiążącymi regułami korporacyjnymi, »odstępstwami« lub »możliwymi przyszłymi odstępstwami« za pomocą kanałów ustanowionych na mocy obowiązujących przepisów i polityki Stanów Zjednoczonych oraz aby ułatwić udzielanie odpowiedzi na te wnioski”.

III. Postępowanie główne, pytania prejudycjalne i postępowanie przed Trybunałem

39. Maximilian Schrems, obywatel austriacki zamieszkały w Austrii, jest użytkownikiem sieci społecznościowej Facebook. Od wszystkich użytkowników tej sieci społecznościowej zamieszkałych na terytorium Unii wymagane jest w chwili rejestracji zawarcie umowy z Facebook Ireland, spółką zależną spółki Facebook Inc. z siedzibą w Stanach Zjednoczonych. Dane osobowe tych użytkowników są w całości lub w części przekazywane na serwery należące do spółki Facebook Inc. położone na terytorium Stanów Zjednoczonych, gdzie dane te są przetwarzane.

40. W dniu 25 czerwca 2013 r. M. Schrems złożył skargę do DPC, w której żądał zasadniczo, aby organ ten zakazał spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych. Podniósł on w swej skardze, że prawo i praktyka obowiązujące w tym państwie trzecim nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed prowadzonymi przez organy władzy publicznej działaniami nadzorczymi. Maximilian Schrems powołał się w tym względzie na ujawnione przez Edwarda Snowdena informacje na temat działalności amerykańskich służb wywiadowczych, a w szczególności służb National Security Agency (NSA) (Krajowej Agencji Bezpieczeństwa, Stany Zjednoczone).

41. Skarga ta została oddalona między innymi na tej podstawie, że wszelkie kwestie dotyczące odpowiedniego charakteru stopnia ochrony zapewnianego w Stanach Zjednoczonych winny być rozstrzygane zgodnie z decyzją w sprawie bezpiecznej przystani. W decyzji tej Komisja stwierdziła, że to państwo trzecie zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych przedsiębiorstwom mającym siedziby na jego terytorium, które zobowiązały się przestrzegać zasad wyrażonych w tej decyzji.

42. Maximilian Schrems zaskarżył decyzję oddalającą jego skargę do High Court (wysokiego trybunału, Irlandia). Sąd ten uznał, że mimo iż M. Schrems formalnie nie zakwestionował ważności decyzji w sprawie bezpiecznej przystani, w rzeczywistości w swojej skardze podważa on zgodność z prawem systemu ustanowionego na mocy tej decyzji. W związku z tym sąd ten zwrócił się do Trybunału z pytaniami zmierzającymi zasadniczo do ustalenia, czy organy władzy państwa członkowskiego odpowiedzialne za ochronę danych osobowych (zwane dalej „organami nadzorczymi”), rozpatrując skargę dotyczącą ochrony praw i wolności osoby w odniesieniu do przetwarzania dotyczących jej danych osobowych, które zostały przekazane do państwa trzeciego, są związane poczynionymi przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46 ustaleniami odnoszącymi się do adekwatności stopnia ochrony zapewnianego przez to państwo trzecie, w sytuacji gdy skarżący kwestionuje te ustalenia.

43. Po ustaleniu w pkt 51 i 52 wyroku Schrems, że decyzja stwierdzająca odpowiedni stopień ochrony wiąże organy nadzorcze dopóki nie zostanie stwierdzona jej nieważność, Trybunał w pkt 63 i 65 tego wyroku orzekł, co następuje:

„63. [...] [j]eśli osoba, której dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego będącego przedmiotem decyzji Komisji przyjętej na mocy art. 25 ust. 6 dyrektywy 95/46, wnosi do krajowego organu nadzorczego skargę dotyczącą ochrony jej praw i wolności w zakresie przetwarzania tych danych i podważa w tej skardze [...], zgodność tej decyzji z ochroną życia prywatnego oraz podstawowych praw i wolności jednostek, to krajowy organ nadzorczy zobowiązany jest do rozpatrzenia tej skargi z wszelką wymaganą starannością.

[...]

65. W [...] sytuacji, w której omawiany organ uzna zarzuty podniesione przez [tę] osobę [...] za zasadne, organ ten powinien – zgodnie z art. 28 ust. 3 akapit pierwszy [tiret trzecie] dyrektywy 95/46 w związku w szczególności z art. 8 ust. 3 karty – mieć prawo pozywania do sądu. W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji”.

44. W omawianym wyroku Trybunał przeanalizował również ważność decyzji w sprawie bezpiecznej przystani w kontekście wymogów wynikających z dyrektywy 95/46 w związku z kartą. W wyniku powyższej analizy Trybunał stwierdził nieważność tej decyzji¹³.

45. W następstwie wydania wyroku Schrems sąd odsyłający uchylił decyzję, na mocy której DPC oddalił skargę M. Schremsa i przekazał tę skargę do ponownego rozpoznania przez DPC. Ten ostatni wszczął postępowanie i zwrócił się do M. Schremsa, aby ten przeformułował skargę z uwagi na stwierdzenie nieważności decyzji w sprawie bezpiecznej przystani.

¹³ Zobacz wyrok Schrems (pkt 106).

46. W tym celu M. Schrems zwrócił się do spółki Facebook Ireland o wskazanie podstaw prawnych dla przekazywania danych osobowych użytkowników sieci społecznościowej Facebook z Unii do Stanów Zjednoczonych. Facebook Ireland, nie wskazując wszystkich podstaw prawnych, na jakich się opiera, powołała się na umowę w sprawie przekazywania i przetwarzania danych (*data transfer processing agreement*) zawartą pomiędzy tą spółką a Facebook Inc., mającą zastosowanie od dnia 20 listopada 2015 r., jak również na decyzję 2010/87.

47. W przeformułowanej skardze M. Schrems podnosi, po pierwsze, że zawarte w tej umowie klauzule nie są zgodne ze standardowymi klauzulami umownymi zawartymi w załączniku do decyzji 2010/87. Po drugie, M. Schrems twierdzi, że te standardowe klauzule umowne w żadnym razie nie mogą stanowić podstawy dla przekazywania jego danych osobowych do Stanów Zjednoczonych. Jest tak dlatego, że prawo amerykańskie wymaga, aby spółka Facebook Inc. udostępniała dane osobowe swoich użytkowników amerykańskim organom, takim jak NSA i Federal Bureau of Investigation (FBI) (federalne biuro śledcze, Stany Zjednoczone) w ramach programów nadzoru, które stoją na przeszkodzie korzystaniu z praw gwarantowanych w art. 7, 8 i 47 karty. Maximilian Schrems zarzuca, że brak jest środków ochrony prawnej, które umożliwiłyby zainteresowanym osobom egzekwowanie ich praw do poszanowania życia prywatnego i do ochrony danych osobowych. W związku z tym wnosi on do DPC o zawieszenie przekazywania tych danych zgodnie z art. 4 decyzji 2010/87.

48. W ramach prowadzonego przez DPC dochodzenia Facebook Ireland przyznała, że w dalszym ciągu przekazuje dane osobowe użytkowników sieci społecznościowej Facebook zamieszkających w Unii do Stanów Zjednoczonych oraz że opiera się ona w tym celu głównie na standardowych klauzulach umownych zawartych w załączniku do decyzji 2010/87.

49. Prowadzone przez DPC dochodzenie miało na celu ustalenie, po pierwsze, czy Stany Zjednoczone zapewniają odpowiednią ochronę danych osobowych obywateli Unii, i, po drugie, gdyby tak nie było, czy decyzje w sprawie standardowych klauzul umownych zapewniają wystarczające gwarancje, jeśli chodzi o ochronę wolności i praw podstawowych tych obywateli.

50. W projekcie decyzji (*draft decision*) DPC uznał w tym względzie wstępnie, że prawo amerykańskie nie oferuje skutecznych środków ochrony prawnej w rozumieniu art. 47 karty, obywatelom Unii, których dane osobowe są przekazywane do Stanów Zjednoczonych, gdzie mogą podlegać przetwarzaniu przez amerykańskie agencje do celów bezpieczeństwa narodowego w sposób niezgodny z art. 7 i 8 karty. Zabezpieczenia ustanowione w klauzulach znajdujących się w załączniku do decyzji w sprawie standardowych klauzul umownych nie wypełniają tej luki, ponieważ nie są one wiążące dla amerykańskich organów lub agencji i przyznają zainteresowanym osobom wyłącznie prawa mające źródło w umowie, których mogą one dochodzić od podmiotu przekazującego dane lub od podmiotu odbierającego dane.

51. W tych okolicznościach DPC uznał, że nie może wydać orzeczenia w przedmiocie skargi M. Schremsa bez zbadania przez Trybunał ważności decyzji w sprawie standardowych klauzul umownych. Zgodnie z tym, co stanowi pkt 65 wyroku Schrems, DPC doprowadził więc do wszczęcia przed sądem odsyłającym postępowania zmierzającego do tego, aby ów sąd, jeżeli podziela wątpliwości DPC, wystąpił do Trybunału z odesłaniem prejudycjalnym dotyczącym ważności tych decyzji.

52. Rząd Stanów Zjednoczonych, Electronic Privacy Information Centre (EPIC), Business Software Alliance (BSA) i Digitaleurope zostali dopuszczeni do udziału w postępowaniu przed sądem odsyłającym w charakterze interwenientów.

53. High Court (wysoki trybunał, Irlandia), aby stwierdzić, czy podziela wyrażone przez DPC wątpliwości co do ważności decyzji w sprawie standardowych klauzul umownych, dopuścił dowody przedstawione przez strony sporu oraz wysłuchał argumentów przedstawionych przez nie i przez interwenientów. Przedmiotem dowodu były w szczególności przepisy prawa Stanów Zjednoczonych, które zostały przedstawione przez biegłych. W prawie irlandzkim, prawo obce uznawane jest za

okoliczność faktyczną, która, tak jak każda inna okoliczność faktyczna, podlega ustaleniu przy pomocy dowodów. W oparciu o te dowody sąd odsyłający dokonał oceny przepisów prawa Stanów Zjednoczonych zezwalających na prowadzenie czynności nadzorczych przez organy i agencje rządowe, funkcjonowania dwóch publicznie znanych programów nadzorczych („PRISM” i „Upstream”), różnych środków prawnych, jakimi dysponują jednostki, których prawa zostały naruszone przez zastosowanie środków nadzorczych oraz zabezpieczeń systemowych i mechanizmów kontroli. Sąd ten zawarł wyniki tej oceny w wyroku z dnia 3 października 2017 r. [zwanym dalej „wyrokiem High Court (wysokiego trybunału) z dnia 3 października 2017 r.”], stanowiącym załącznik do postanowienia odsyłającego.

54. W wyroku tym sąd odsyłający, wśród podstaw prawnych zezwalających na przechwytywanie zagranicznych wiadomości przez amerykańskie służby wywiadowcze, wymienił art. 702 Foreign Intelligence and Surveillance Act (FISA) (ustawy o nadzorze w dziedzinie wywiadu zagranicznego) oraz Executive Order 12333 (dekret prezydencki nr 12333, zwany dalej „EO 12333”).

55. Zgodnie z ustaleniami dokonanymi w tym wyroku art. 702 FISA upoważnia Attorney General (prokuratora generalnego, Stany Zjednoczone) i Director of National Intelligence (DNI) (dyrektora państwowych służb wywiadu, Stany Zjednoczone) działających łącznie, do wydania na okres jednego roku (w celu pozyskiwania zagranicznych informacji wywiadowczych) zezwolenia na prowadzenie czynności nadzorczych wobec osób, które nie są obywatelami amerykańskimi ani nie zamieszkują na stałe w Stanach Zjednoczonych (tzw. „osoby niebędące obywatelami ani rezydentami amerykańskimi”), gdy można racjonalnie założyć, że przebywają one poza terytorium Stanów Zjednoczonych¹⁴. Zgodnie z FISA pojęcie „zagranicznych informacji wywiadowczych” oznacza informacje dotyczące możliwości rządu w zakresie zabezpieczenia się przed atakami z zewnątrz, terroryzmu, rozprzestrzeniania broni masowego rażenia oraz prowadzenia przez Stany Zjednoczone polityki zagranicznej¹⁵.

56. Powyższe roczne zezwolenia, podobnie jak procedury regulujące namierzanie osób poddawanych nadzorowi oraz przetwarzanie („minimalizację”) zebranych informacji¹⁶, wymagają wydania zgody przez Foreign Intelligence Surveillance Court (FISC) (sąd ds. nadzoru nad obcym wywiadem, Stany Zjednoczone). O ile „tradycyjny” nadzór prowadzony na podstawie innych przepisów FISA wymaga wykazania „prawdopodobnej przyczyny” pozwalającej podejrzewać, że namierzane osoby mają związki z obcym mocarstwem lub są jego agentami, to prowadzenie nadzoru na podstawie art. 702 FISA nie jest uzależnione ani od wykazania takiej „prawdopodobnej przyczyny”, ani od udzielenia przez FISC zgody na namierzanie określonych osób. Ponadto – również zgodnie z ustaleniami sądu odsyłającego – procedury minimalizacji nie mają zastosowania w stosunku do osób niebędących obywatelami ani rezydentami amerykańskimi przebywających poza Stanami Zjednoczonymi.

57. W praktyce po udzieleniu zgody przez FISC NSA przesyła dostawcom usług łączności elektronicznej mającym siedziby w Stanach Zjednoczonych wytyczne zawierające kryteria wyszukiwania nazywane „selektorami”, skojarzone z namierzanymi osobami (takie jak numery telefonu czy adresy poczty elektronicznej). Dostawcy ci są wtedy obowiązani do przekazywania NSA danych zgodnych z selektorami oraz do zachowania w tajemnicy wytycznych, które otrzymali. Mają oni możliwość wniesienia skargi do FISC w celu zmiany lub uchylenia wytycznej NSA. Od orzeczenia FISC przysługuje apelacja do Intelligence Surveillance Court of Review (FISCR) (sąd rozpatrujący środki odwoławcze od orzeczeń w sprawach nadzoru nad wywiadem zagranicznym, Stany Zjednoczone).

¹⁴ 50 U.S.C. 1881 (a).

¹⁵ 50 U.S.C. 1881 (e).

¹⁶ Sąd odsyłający stwierdził, że procedury namierzania dotyczą sposobu, w jaki władza wykonawcza określa, czy można racjonalnie uznać, że dana jednostka jest osobą niebędącą obywatelem lub rezydentem amerykańskim przebywającym poza terytorium Stanów Zjednoczonych oraz czy namierzanie tej osoby może doprowadzić do pozyskania zagranicznych informacji wywiadowczych. Procedury minimalizacji obejmują pozyskiwanie, gromadzenie, wykorzystanie i rozpowszechnianie wszelkich nieupublicznych informacji dotyczących obywateli amerykańskich, pozyskanych na podstawie art. 702 FISA.

58. High Court (wysoki trybunał, Irlandia) stwierdził, że podstawę prawną programów PRISM i Upstream stanowi art. 702 FISA.

59. W ramach programu PRISM dostawcy usług łączności elektronicznej obowiązani są przekazywać do NSA wszystkie komunikaty „wychodzące z” lub „przychodzące do” selektora przekazanego przez tę agencję. Część komunikatów jest przekazywana do FBI oraz do Central Intelligence Agency (CIA) (centralnej agencji wywiadowczej, Stany Zjednoczone). W 2015 r. nadzorem było objętych 94 386 osób, a w 2011 r. rząd Stanów Zjednoczonych pozyskał w ramach tego programu ponad 250 milionów komunikatów.

60. Program Upstream polega na świadczeniu obowiązkowego wsparcia przez przedsiębiorstwa korzystające z „infrastruktury szkieletowej” – czyli sieci kabli, przełączników sieciowych i ruterów – w ramach której odbywa się tranzyt komunikatów telefonicznych i komunikatów internetowych. Przedsiębiorstwa te mają obowiązek umożliwienia NSA kopiowania i filtrowania internetowego ruchu danych w celu pozyskiwania komunikatów „wychodzących z”, „przychodzących do” lub „dotyczących” selektora wskazanego w wytycznych tej agencji. Komunikaty „dotyczące” danego selektora są to komunikaty, które odnoszą się do tego selektora, przy czym osoba niebędąca obywatelem ani rezydentem amerykańskim skojarzona z tym selektorem nie musi koniecznie uczestniczyć w komunikacji. Choć z opinii FISC z dnia 26 kwietnia 2017 r. wynika, że począwszy od tej daty rząd amerykański już nie gromadzi i nie pozyskuje komunikatów „dotyczących” selektora, opinia ta nie świadczy o tym, że NSA zaprzestała kopiowania i filtrowania komunikatów w trakcie ich tranzytu przez jej własne urządzenia służące do inwigilacji. Program Upstream zakłada zatem udzielanie NSA dostępu zarówno do metadanych, jak i do treści komunikatów. Od 2011 r. NSA gromadzi w ramach programu Upstream około 26,5 mln komunikatów rocznie, co jednakże stanowi tylko niewielką część komunikatów poddanych procesowi filtrowania, jaki odbywa się w ramach tego programu.

61. Poza tym, zgodnie z ustaleniami High Court (wysokiego trybunału, Irlandia), EO 12333 zezwala na sprawowanie nadzoru nad komunikatami elektronicznymi poza terytorium Stanów Zjednoczonych, umożliwiając (dla celów wywiadu zagranicznego) uzyskanie dostępu do danych, które bądź to są „w tranzycie” w kierunku tego terytorium, bądź też odbywają „tranzyt” przez to terytorium, lecz nie mają podlegać na nim przetwarzaniu, oraz zbieranie i przechowywanie tych danych. EO 12333 definiuje pojęcie „zagranicznych informacji wywiadowczych” jako obejmujące informacje, które dotyczą możliwości, zamiarów lub działalności obcych rządów, zagranicznych organizacji lub cudzoziemców¹⁷.

62. EO 12333 umożliwia NSA uzyskanie dostępu do podwodnych kabli ułożonych na dnie Oceanu Atlantyckiego, przy pomocy których dane są przekazywane z Unii do Stanów Zjednoczonych, jeszcze zanim dane te dotrą do Stanów Zjednoczonych i zostaną z tego względu objęte przepisami FISA. Brak jest jednak dowodów na to, że na podstawie tego dekretu prezydenckiego został wprowadzony w życie jakikolwiek program.

63. Mimo, że EO 12333 przewiduje ograniczenia dotyczące zbierania, zatrzymywania i rozpowszechniania informacji, ograniczenia te nie mają zastosowania w przypadku osób niebędących obywatelami ani rezydentami amerykańskimi. Tym ostatnim przysługują wyłącznie gwarancje sformułowane w Presidential Policy Directive 28 (strategicznej dyrektywie prezydenckiej nr 28, zwanej dalej „PPD 28”), która ma zastosowanie do wszelkiej działalności polegającej na zbieraniu i wykorzystaniu zagranicznych informacji wywiadowczych pochodzenia elektromagnetycznego. PPD 28 stanowi, że poszanowanie życia prywatnego należy do względów, jakie należy brać pod uwagę przy planowaniu tej działalności, że jedynym celem zbierania danych może być pozyskiwanie zagranicznych informacji wywiadowczych i kontrwywiadowczych oraz że proces ten powinien być „w naj „w jak największym stopniu dostosowany do indywidualnych potrzeb”.

¹⁷ EO 12333, pkt 3.5 lit. e).

64. Zdaniem sądu odsyłającego czynności NSA oparte na EO 12333, który w każdej chwili może być zmieniony lub uchylony przez prezydenta Stanów Zjednoczonych, nie są regulowane prawem, nie podlegają kontroli sądowej i nie mogą zostać zaskarżone do sądu.

65. Na podstawie powyższych ustaleń sąd ten uznaje, że Stany Zjednoczone przetwarzają dane osobowe na skalę masową i bez rozróżnienia, co może narażać osoby, których to dotyczy, na ryzyko naruszenia praw przysługujących im na podstawie art. 7 i 8 karty.

66. Co więcej, sąd ten wskazuje, że obywatele Unii nie mają dostępu do tych samych co obywatele amerykańscy sądowych środków ochrony prawnej przed niezgodnym z prawem przetwarzaniem ich danych osobowych przez organy amerykańskie. Czwarta poprawka do konstytucji Stanów Zjednoczonych, która jego zdaniem stanowi najważniejszy środek ochrony przed prowadzeniem niezgodnego z prawem nadzoru, nie ma zastosowania w przypadku obywateli Unii, których nie łączą dobrowolne i istotne więzi ze Stanami Zjednoczonymi. Nawet jeżeli tym obywatelom przysługują pewne inne środki prawne, to korzystanie z nich wiąże się z istotnymi utrudnieniami.

67. W szczególności art. III konstytucji Stanów Zjednoczonych uzależnia możliwość skorzystania ze środków ochrony prawnej przed sądami federalnymi od wykazania legitymacji procesowej (*standing*) przez zainteresowaną osobę. Przysługiwanie tej legitymacji procesowej jest uzależnione w szczególności od wykazania przez tę osobę poniesienia rzeczywistej szkody, która, po pierwsze, jest konkretna i zindywidualizowana, i, po drugie, doszło już do jej wyrządzenia lub jest ono nieuchronne. Powołując się między innymi na wyrok Supreme Court of the United States (sądu najwyższego Stanów Zjednoczonych), *Clapper przeciwko Amnesty International US*¹⁸, sąd odsyłający uważa, że ten warunek jest praktyce nadmiernie trudny do spełnienia, w szczególności ze względu na brak obowiązku informowania osób, których dane dotyczą, o zastosowanych w stosunku do nich środkach nadzorczych¹⁹. Część środków ochrony prawnej, jakimi dysponują obywatele Unii, jest poza tym uzależniona od spełnienia innych ograniczających warunków, takich jak konieczność wykazania szkody o charakterze majątkowym. Immunitet państwowy, z którego korzystają agencje wywiadu, oraz objęcie omawianych informacji klauzulami tajności, także stanowią przeszkodę w korzystaniu z niektórych środków ochrony prawnej²⁰.

68. High Court (wysoki trybunał, Irlandia) wymienia ponadto różne mechanizmy służące kontroli i nadzoru nad działalnością agencji wywiadowczych.

69. Znajduje się wśród nich, po pierwsze, mechanizm corocznego zatwierdzania przez FISC programów mających za podstawę art. 702 FISA, przy czym jednak w ramach tego mechanizmu FISC nie zatwierdza poszczególnych selektorów. Poza tym, zbieranie zagranicznych informacji wywiadowczych na podstawie EO 12333 nie jest poprzedzone jakąkolwiek kontrolą sądową.

70. Po drugie, sąd odsyłający wymienia kilka pozasądowych mechanizmów nadzoru nad działalnością wywiadowczą. Wskazuje on w szczególności na rolę odgrywaną przez Inspectors General (inspektorów generalnych, Stany Zjednoczone), którzy w ramach każdej agencji wywiadowczej odpowiadają za nadzór nad działalnością wywiadowczą. Poza tym, Privacy and Civil Liberties Oversight Board (zwana dalej „PCLOB”) (rada nadzorująca kwestie prywatności i praw obywatelskich, Stany Zjednoczone), będąca niezależną agencją w ramach władzy wykonawczej, otrzymuje sprawozdania od wyznaczonych w każdej agencji urzędników odpowiedzialnych za kwestie praw obywatelskich lub prywatności (*civil*

18 133 S.Ct. 1138 (2013).

19 Sąd odsyłający stwierdził jednak, że od zasady, zgodnie z którą nie ma wymogu zawiadamiania osoby objętej środkami nadzorczymi, istnieje wyjątek w sytuacji, gdy rząd amerykański zamierza wykorzystać dane zebrane na podstawie art. 702 FISA przeciwko tej osobie w ramach postępowania karnego lub administracyjnego.

20 Sąd odsyłający zauważył w szczególności, że mimo iż Judicial Redress Act (JRA) (ustawa w sprawie ochrony sądowej) objęła obywateli Unii przepisami Privacy Act (ustawy w sprawie ochrony prywatności), która umożliwia osobom fizycznym uzyskanie dostępu do dotyczących ich informacji znajdujących się w posiadaniu niektórych agencji w związku z pewnymi państwami trzecimi, NSA nie znajduje się wśród agencji wskazanych w JRA.

liberties or privacy officers). PCLOB sporządza regularnie sprawozdania przeznaczone dla komisji Kongresu i dla prezydenta. Agencje, których to dotyczy, obowiązane są raportować, między innymi do DNI, o incydentach związanych z naruszeniem zasad i procedur rządzących zbieraniem informacji przez wywiad zagraniczny. Incydenty takie są również raportowane do FISC. Za kontrolę działalności wywiadu zagranicznego odpowiada także Kongres Stanów Zjednoczonych za pośrednictwem komisji ds. wywiadu w Izbie Reprezentantów i Senacie.

71. Jednakże High Court (wysoki trybunał, Irlandia) podkreśla podstawową różnicę między zasadami służącymi zapewnieniu, aby dane były pozyskiwane w sposób legalny oraz aby (gdy zostaną już pozyskane) nie były wykorzystywane w sposób mający znamiona nadużycia, z jednej strony, a dostępnymi środkami ochrony prawnej na wypadek naruszenia tych zasad, z drugiej strony. Ochrona praw podstawowych osób, których dane dotyczą, może być zapewniona wyłącznie wówczas, gdy skuteczne środki ochrony prawnej umożliwiają im dochodzenie ich praw w przypadku naruszenia rzeczonych zasad.

72. W tych okolicznościach sąd odsyłający uznaje zasadność podniesionych przez DPC argumentów, zgodnie z którymi ograniczenia, jakie nakłada amerykańskie prawo na środki ochrony prawnej przysługujące osobom, których dane są przekazywane z Unii, naruszają zasadniczą treść prawa gwarantowanego przez art. 47 karty i w każdym razie stanowią nieproporcjonalną ingerencję w korzystanie z tego prawa.

73. Zdaniem High Court (wysokiego trybunału, Irlandia) oceny tej nie podważa fakt wprowadzenia przez rząd Stanów Zjednoczonych mechanizmu mediacji opisanego w decyzji w sprawie Tarczy Prywatności. Podkreśliwszy, że mechanizm ten jest dostępny dla obywateli Unii, którzy na podstawie racjonalnych przesłanek uważają, że ich dane osobowe zostały przekazane zgodnie z decyzjami w sprawie standardowych klauzul umownych²¹, sąd ten zwrócił uwagę, że rzecznik nie jest sądem spełniającym wymogi wynikające z art. 47 karty, a w szczególności nie jest niezawisły względem władzy wykonawczej²². Sąd ten ma również wątpliwości, czy interwencja ze strony rzecznika, którego decyzje nie podlegają zaskarżeniu do sądu, jest skutecznym środkiem ochrony prawnej. Jego udział nie umożliwia bowiem osobom, których dane osobowe były zbierane, przetwarzane lub udostępniane w sposób niezgodny z prawem, uzyskania odszkodowania lub nakazu zaprzestania niezgodnych z prawem działań, skoro rzecznik nie potwierdza ani nie zaprzecza, że względem skarżącego był stosowany środek elektronicznego nadzoru.

74. Po przedstawieniu swoich wątpliwości co do istnienia merytorycznej równoważności gwarancji przewidzianych w prawie amerykańskim i wymogów wynikających z art. 7, 8 i 47 karty, sąd odsyłający wyraził wątpliwość dotyczącą tego, czy zawarte w decyzjach w sprawie standardowych klauzul umownych standardowe klauzule umowne – które, ze względu na ich charakter, nie są wiążące dla amerykańskich organów władzy – mogą jednak zapewnić ochronę praw podstawowych osób, których dane dotyczą. Sąd ten stwierdził, że podziela wątpliwości DPC co do ważności tych decyzji.

75. W tym względzie sąd odsyłający uważa w szczególności, że art. 28 ust. 3 dyrektywy 95/46, do którego odwołuje się art. 4 decyzji 2010/87, przyznając organom nadzorczym uprawnienie do zawieszenia lub zakazania przekazywania danych na podstawie standardowych klauzul umownych przewidzianych w tej decyzji, nie jest wystarczający, aby rozwiązać te wątpliwości. Poza tym, że, zdaniem sądu odsyłającego, uprawnienie to ma jedynie charakter uznaniowy, sąd ten zastanawia się, w związku z motywem 11 decyzji 2010/87, czy istnieje możliwość wykonania tego uprawnienia w sytuacji, gdy

21 Sąd odsyłający powołuje się w tym względzie na załącznik III A do decyzji w sprawie Tarczy Prywatności (zob. pkt 37 i 38 niniejszej opinii).

22 Sąd odsyłający powołuje się na wyrok z dnia 27 stycznia 2005 r., Denuit i Cordenier (C-125/04, EU:C:2005:69, pkt 12).

stwierdzone uchybienia nie odnoszą się do pojedynczego, wyjątkowego przypadku, lecz mają charakter powszechny i systemowy²³. Sąd odsyłający uważa również, że prawdopodobieństwo wydania w różnych państwach członkowskich rozbieżnych decyzji może przemawiać przeciwko powierzeniu organom nadzorczym obowiązków w zakresie stwierdzania takich uchybień.

76. W tych okolicznościach High Court (wysoki trybunał), orzeczeniem z dnia 4 maja 2018 r.²⁴, które wpłynęło do Trybunału w dniu 9 maja 2018 r., zawiesił postępowanie i zwrócił się do Trybunału z następującymi pytaniami prejudycjalnymi:

- „1) W sytuacji, gdy dane osobowe są przekazywane przez prywatne przedsiębiorstwo z państwa członkowskiego [Unii] do prywatnego przedsiębiorstwa w państwie trzecim w celach komercyjnych na podstawie [decyzji 2010/87] i mogą być dalej przetwarzane w tym państwie trzecim przez jego organy dla celów bezpieczeństwa narodowego, ale także dla celów egzekwowania prawa [utrzymania porządku publicznego] i prowadzenia spraw zagranicznych w tym kraju [państwie] trzecim, czy prawo [Unii] (w tym także karta) ma zastosowanie do przekazywania danych niezależnie od postanowień art. 4 ust. 2 TUE w odniesieniu do bezpieczeństwa narodowego i od postanowień art. 3 ust. 2 tiret pierwsze [dyrektywy 95/46] w odniesieniu do bezpieczeństwa publicznego, obronności i bezpieczeństwa państwa?
- 2) a) Aby określić, czy przekazywanie danych w oparciu o [decyzję 2010/87] z [Unii] do państwa trzeciego, gdzie mogą one być dalej przetwarzane dla celów bezpieczeństwa narodowego, stanowi naruszenie praw jednostki, właściwym punktem odniesienia dla celów dyrektywy [95/46] jest:
- (i) karta, TUE, TFUE, dyrektywa [95/46], [europejska Konwencja o ochronie praw człowieka i podstawowych wolności, podpisana w Rzymie w dniu 4 listopada 1950 r. (zwana dalej „EKPC”).] (czy też jakikolwiek inny przepis prawa Unii); czy
- (ii) prawa krajowe jednego lub większej liczby państw członkowskich?
- b) Jeżeli właściwym punktem odniesienia jest określony w (ii), czy obejmuje on także praktyki w kontekście bezpieczeństwa narodowego w jednym lub większej liczbie państw członkowskich?
- 3) Przy ocenie, czy państwo trzecie zapewnia poziom ochrony wymagany przez prawo [Unii] dla danych osobowych przekazywanych do tego państwa w rozumieniu art. 26 dyrektywy [95/46], czy poziom ochrony w państwie trzecim powinien być oceniany poprzez odniesienie do:
- a) obowiązujących przepisów w państwie trzecim, wynikających z jego prawa krajowego lub zobowiązań międzynarodowych oraz z praktyk mających na celu zapewnienie zgodności z tymi przepisami, zasad wykonywania zawodu i środków bezpieczeństwa, które są przestrzegane w tym państwie trzecim;

23 Motyw 11 decyzji 2010/87 ma następujące brzmienie: „Organy nadzorcze państw członkowskich odgrywają kluczową rolę w tym mechanizmie umownym, zapewniając odpowiednią ochronę danych osobowych po przekazaniu. W wyjątkowych przypadkach, jeżeli podmioty przekazujące dane odmawiają poinstruowania podmiotów odbierających dane lub nie są w stanie tego zrobić we właściwy sposób, co wiąże się z bezpośrednim ryzykiem poważnej szkody dla osób, których dane dotyczą, standardowe klauzule umowne powinny umożliwiać organom nadzorczym kontrolę podmiotów odbierających dane i podwykonawców przetwarzania danych oraz, w stosownych przypadkach, podjęcie decyzji wiążących dla podmiotów odbierających dane i podwykonawców przetwarzania danych. Organy nadzorcze powinny być uprawnione do zakazania lub zawieszenia operacji przekazania danych lub zbioru takich operacji wykonywanych na podstawie standardowych klauzul umownych w tych wyjątkowych przypadkach, w których ustalono, że przekazanie na podstawie umowy może mieć istotne negatywne skutki w odniesieniu do gwarancji i obowiązków zapewniających odpowiednią ochronę osób, których dane dotyczą”.

24 Facebook Ireland zaskarżyła orzeczenie odsyłające do Supreme Court (sąd najwyższy, Irlandia). Środek ten został oddalony wyrokiem z dnia 31 maja 2019 r., The Data Protection Commissioner przeciwko Facebook Ireland Limited and Maximilian Schrems, Appeal n° 2018/68 [zwanym dalej „wyrokiem Supreme Court (sądu najwyższego) z dnia 31 maja 2019 r.”].

czy

- b) przepisów, o których mowa w lit. a) wraz z praktykami administracyjnymi, regulacyjnymi i praktykami w zakresie zgodności oraz polityką w zakresie środków bezpieczeństwa, procedurami, protokołami, mechanizmami kontroli i systemami pozasądowego rozstrzygania sporów istniejącymi w tym państwie trzecim?
- 4) Przy uwzględnieniu stanu faktycznego ustalonego przez High Court (wysoki trybunał) w odniesieniu do prawa Stanów Zjednoczonych, czy przekazywanie danych osobowych z [Unii] do Stanów Zjednoczonych na podstawie decyzji [2010/87] narusza prawa osób fizycznych wynikające z art. 7 lub 8 karty?
- 5) Przy uwzględnieniu stanu faktycznego ustalonego przez High Court (wysoki trybunał) w odniesieniu do prawa Stanów Zjednoczonych, jeżeli dane osobowe są przekazywane z [Unii] do Stanów Zjednoczonych na podstawie decyzji [2010/87]:
 - a) Czy poziom ochrony w prawie Stanów Zjednoczonych zapewnia poszanowanie istoty prawa osób fizycznych do korzystania z sądowych środków ochrony prawnej w związku z naruszeniem ich prawa do poufności danych osobowych zagwarantowanych przez art. 47 karty?

Jeżeli odpowiedź na pytanie a) jest twierdząca:

- b) Czy ograniczenia, jakie nakłada prawo Stanów Zjednoczonych na prawo jednostki do korzystania z sądowych środków ochrony prawnej w kontekście bezpieczeństwa narodowego Stanów Zjednoczonych, są proporcjonalne w rozumieniu art. 52 karty i nie wykraczają poza to, co jest niezbędne w społeczeństwie demokratycznym dla celów bezpieczeństwa narodowego?
- 6) a) W świetle przepisów dyrektywy [95/46], a w szczególności jej art. 25 i 26 interpretowanych w świetle karty, jaki poziom ochrony należy zapewnić przy przekazywaniu danych osobowych do państwa trzeciego na podstawie standardowych klauzul umownych przyjętych zgodnie z decyzją Komisji w oparciu o art. 26 ust. 4 [tej dyrektywy]?
- b) Jakie kwestie należy wziąć pod uwagę przy ocenie, czy poziom ochrony danych osobowych przekazywanych do państwa trzeciego na podstawie decyzji [2010/87] spełnia wymogi dyrektywy [95/46] i karty?
- 7) Czy okoliczność, że standardowe klauzule umowne obowiązują pomiędzy podmiotem przekazującym a odbierającym dane i nie są wiążące dla władz krajowych państwa trzeciego, które mogą wymagać od podmiotu odbierającego dane udostępniania jego służbom bezpieczeństwa w celu dalszego przetwarzania danych osobowych przekazywanych na mocy klauzul przewidzianych w decyzji [2010/87], wyklucza zapewnienie przez te klauzule odpowiednich zabezpieczeń zgodnie z art. 26 ust. 2 dyrektywy [95/46]?
- 8) Jeżeli podmiot odbierający dane w państwie trzecim jest objęty przepisami dotyczącymi nadzoru, które zdaniem [organu nadzorczego] są sprzeczne ze standardowymi klauzulami umownymi lub z art. 25 i 26 dyrektywy [95/46] lub z kartą, czy [organ nadzorczy] jest zobowiązany do skorzystania ze swoich uprawnień wykonawczych zgodnie z art. 28 ust. 3 dyrektywy [95/46] w celu zawieszenia przepływu danych, czy też wykonywanie tych uprawnień jest ograniczone do sytuacji wyjątkowych, w świetle motywu 11 [decyzji 2010/87], względnie czy [organ nadzorczy] w ramach swobodnego uznania może nie zawieszać przepływu danych?

- 9) a) Dla celów art. 25 ust. 6 dyrektywy [95/46], czy decyzja [w sprawie Tarczy Prywatności] stanowi ustalenie o powszechnym zastosowaniu wiążące dla [organów nadzorczych] oraz sądów państw członkowskich stwierdzające, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony w rozumieniu art. 25 ust. 2 dyrektywy [95/46], co wynika z prawa krajowego Stanów Zjednoczonych lub z międzynarodowych zobowiązań, jakie państwo to przyjęło?
- b) Jeżeli nie, jakie znaczenie, jeśli w ogóle, ma decyzja [w sprawie Tarczy Prywatności] przy prowadzeniu oceny adekwatności zabezpieczeń przewidzianych dla danych przekazywanych do Stanów Zjednoczonych na mocy decyzji [2010/87]?
- 10) Przy uwzględnieniu ustaleń High Court (wysokiego trybunału) w odniesieniu do prawa Stanów Zjednoczonych, czy powołanie Rzecznika ds. Tarczy Prywatności zgodnie z [załącznikiem III A] do decyzji w sprawie Tarczy Prywatności, w związku z istniejącym systemem w Stanach Zjednoczonych zapewnia, że prawo Stanów Zjednoczonych przewiduje środek ochrony prawnej dla osób, których dane osobowe są przekazywane do Stanów Zjednoczonych na podstawie decyzji [2010/87], zgodny z art. 47 karty?
- 11) Czy decyzja [2010/87] narusza art. 7, 8 lub 47 karty?”.

77. DPC, Facebook Ireland, M. Schrems, rząd Stanów Zjednoczonych, EPIC, BSA, Digitaleurope, Irlandia, rządy niemiecki, niderlandzki, austriacki, polski, portugalski i Zjednoczonego Królestwa, Parlament Europejski i Komisja przedstawili przed Trybunałem uwagi na piśmie. DPC, Facebook Ireland, M. Schrems, rząd Stanów Zjednoczonych, EPIC, BSA, Digitaleurope, Irlandia, rządy belgijski, czeski, niemiecki, francuski, niderlandzki, austriacki i Zjednoczonego Królestwa, Parlament, Komisja oraz Europejska Rada Ochrony Danych (European Data Protection Board, EROD) byli reprezentowani podczas rozprawy, która odbyła się w dniu 9 lipca 2019 r.

IV. Analiza

A. Uwagi wstępne

78. W wyniku stwierdzenia przez Trybunał w wyroku Schrems nieważności decyzji w sprawie bezpiecznej przystani przekazywanie danych osobowych do Stanów Zjednoczonych było kontynuowane w oparciu o inne podstawy prawne. Spółki przekazujące dane mogły w szczególności zawierać z podmiotami odbierającymi dane umowy zawierające standardowe klauzule opracowane przez Komisję. Klauzule te służą również za podstawę prawną przekazywania danych do wielu innych państw trzecich, w stosunku do których Komisja nie przyjęła decyzji stwierdzającej odpowiedni stopień ochrony²⁵. Decyzja w sprawie Tarczy Prywatności umożliwia obecnie przedsiębiorstwom, które przyjęły zasady wyrażone w tej decyzji w drodze samocertyfikacji, przekazywanie danych osobowych do Stanów Zjednoczonych bez żadnych innych formalności.

²⁵ BSA twierdzi, że 70% z przedsiębiorstw członkowskich tego stowarzyszenia, które udzieliły odpowiedzi na ankietę dotyczącą tej kwestii oświadczyło, iż korzysta ze standardowych klauzul umownych jako głównej podstawy prawnej przekazywania danych osobowych do państw trzecich. Digitaleurope także twierdzi, że standardowe klauzule umowne stanowią główny instrument prawny wskazywany jako podstawa przekazywania danych.

79. Jak wynika jednoznacznie z postanowienia odsyłającego i jak podkreślili BSA, Digitaleurope, Irlandia, rządy austriacki i francuski, Parlament i Komisja, zawisły przed High Court (wysokim trybunałem) spór w postępowaniu głównym dotyczy wyłącznie ustalenia, czy decyzja, na mocy której Komisja wprowadziła standardowe klauzule umowne powoływane jako podstawa przekazywania danych, o których mowa w skardze M. Schremsa, a mianowicie decyzja 2010/87²⁶, jest ważna.

80. Spór ten został zapoczątkowany skargą, w drodze której DPC zwrócił się do sądu odsyłającego, aby ten skierował do Trybunału pytanie prejudycjalne odnoszące się do ważności decyzji 2010/87. Sąd odsyłający twierdzi, że w związku z tym spór w postępowaniu głównym dotyczy korzystania ze środka ochrony prawnej, do ustanowienia którego Trybunał zobowiązał państwa członkowskie w pkt 65 wyroku Schrems.

81. Dla przypomnienia, Trybunał w pkt 63 tego wyroku orzekł, że organ nadzorczy obowiązany jest rozpatrzyć z wszelką wymaganą starannością skargę, w której osoba, której dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego będącego przedmiotem decyzji stwierdzającej odpowiedni stopień ochrony, kwestionuje zgodność tej decyzji z prawami podstawowymi ustanowionymi w karcie. Zgodnie z pkt 65 omawianego wyroku, w sytuacji, w której organ ten uzna zarzuty podniesione w tej skardze za zasadne, powinien on – zgodnie z art. 28 ust. 3 akapit pierwszy tiret trzecie dyrektywy 95/46 (którego odpowiednikiem jest art. 58 ust. 5 RODO) w związku z art. 8 ust. 3 karty – mieć prawo pozywania do sądu. W tym względzie do krajowego ustawodawcy należy ustanowienie środków ochrony prawnej umożliwiających temu organowi podniesienie zarzutów przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości rzeczonego organu, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności rozpatrywanej decyzji.

82. Podobnie jak sąd odsyłający uważam, że powyższe wnioski mają zastosowanie w drodze analogii do sytuacji, gdy organ nadzorczy, w związku z rozpatrywaniem wniesionej doń skargi, nie ma wątpliwości co do ważności decyzji stwierdzającej odpowiedni stopień ochrony, lecz co do ważności decyzji takiej jak decyzja 2010/87, wprowadzającej standardowe klauzule umowne na potrzeby przekazywania danych osobowych do państw trzecich. Wbrew temu, co twierdzi rząd niemiecki, bez znaczenia jest to, czy te wątpliwości odpowiadają zarzutom podniesionym przed tym organem przez skarżącego, czy też organ ten zakwestionował ważność danej decyzji ze swej własnej inicjatywy. Wymogi wynikające z art. 58 ust. 5 RODO i z art. 8 ust. 3 karty, na których opiera się przedstawione przez Trybunał uzasadnienie, mają bowiem zastosowanie niezależnie od podstawy prawnej przekazywania danych, którego dotyczy skarga wniesiona do organu nadzorczego i powodów, dla których organ ten ma wątpliwości co do ważności decyzji analizowanej w ramach rozpatrywania tej skargi.

83. Uściślwszy powyższe, należy wskazać, że wystąpienie przez DPC do sądu odsyłającego, aby ten zadał Trybunałowi pytanie o ważność decyzji 2010/87, jest umotywowane tym, że DPC uważa, iż udzielenie przez Trybunał wyjaśnień w tym przedmiocie jest niezbędne dla rozpatrzenia skargi, w której M. Schrems żąda, aby organ ten skorzystał z uprawnienia, jakim dysponuje na mocy art. 28 ust. 3 tiret drugie dyrektywy 95/46 – i które obecnie przyznaje mu art. 58 ust. 2 lit. f) RODO – do zawieszenia przekazywania dotyczących go danych osobowych przez Facebook Ireland do Facebook Inc.

26 Chociaż sąd odsyłający wskazuje, że wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy ważności trzech decyzji w sprawie standardowych klauzul umownych, ponieważ były one analizowane w projekcie decyzji DPC i w wyroku z dnia 3 października 2017 r., pytania prejudycjalne odnoszą się wyłącznie do decyzji 2010/87. Jest tak dlatego, że Facebook Ireland wskazała sądowi tę decyzję jako podstawę prawną przekazywania danych osobowych europejskich użytkowników sieci społecznościowej Facebook do Stanów Zjednoczonych. Moja analiza będzie więc dotyczyła tylko tej decyzji.

84. W związku z tym, chociaż spór w postępowaniu głównym dotyczy wyłącznie ważności decyzji 2010/87 *in abstracto*, leżące u podstaw tego sporu postępowanie przed DPC wiąże się ze skorzystaniem przez ten organ w *konkretnym przypadku* z przysługujących mu uprawnień naprawczych. Zaproponuję Trybunałowi, aby ograniczył się do przeprowadzenia analizy przedłożonych pytań w zakresie niezbędnym do wydania orzeczenia co do ważności decyzji 2010/87, ponieważ taka analiza jest wystarczająca do tego, aby umożliwić sądowi odsyłającemu rozstrzygnięcie zawisłego przed nim sporu²⁷.

85. Przed dokonaniem oceny ważności tej decyzji należy oddalić pewne zastrzeżenia podniesione względem dopuszczalności wniosku o wydanie orzeczenia w trybie prejudycjalnym.

B. W przedmiocie dopuszczalności odesłania prejudycjalnego

86. Dopuszczalność wniosku o wydanie orzeczenia w trybie prejudycjalnym była kwestionowana z różnych powodów związanych zasadniczo z brakiem zastosowania *ratione temporis* dyrektywy 95/46, której dotyczą pytania prejudycjalne (część 1), z okolicznością, że postępowanie przed DPC nie znajduje się na dostatecznie zaawansowanym etapie, aby uzasadnić użyteczność takiego wniosku (część 2) oraz z istnieniem niepewności odnoszących się do okoliczności faktycznych opisanych przez sąd odsyłający (część 3).

87. Odpowiem na powyższe zarzuty niedopuszczalności nie zapominając o domniemaniu, zgodnie z którym pytania przedłożone Trybunałowi na podstawie art. 267 TFUE mają znaczenie dla sprawy. Zgodnie z utrwalonym orzecnictwem, Trybunał może odmówić rozstrzygnięcia w przedmiocie postawionego przez sąd krajowy pytania prejudycjalnego tylko wtedy, gdy oczywiste jest, że wykładnia przepisu prawa Unii, o którą się zwrócono, nie ma żadnego związku ze stanem faktycznym lub z przedmiotem sporu w postępowaniu głównym, gdy problem jest natury hipotetycznej bądź gdy Trybunał nie dysponuje informacjami w zakresie stanu faktycznego lub prawnego, które są niezbędne do udzielenia przydatnej odpowiedzi na przedstawione mu pytania²⁸.

1. W przedmiocie stosowania dyrektywy 95/46 *ratione temporis*

88. Facebook Ireland twierdzi, że pytania prejudycjalne są niedopuszczalne, ponieważ odnoszą się do dyrektywy 95/46, podczas gdy dyrektywa ta została uchylona i zastąpiona przez RODO ze skutkiem od dnia 25 maja 2018 r.²⁹..

89. Podzielam punkt widzenia, zgodnie z którym ważność decyzji 2010/87 należy rozpatrywać w świetle przepisów RODO.

90. Zgodnie z art. 94 ust. 2 tego rozporządzenia, „[o]desłania do uchylonej dyrektywy należy traktować jako odesłania do [rzeczonego rozporządzenia]”. Wynika z tego, jak się wydaje, że w przypadku gdy decyzja 2010/87 wskazuje jako podstawę prawną art. 26 ust. 4 dyrektywy 95/46, należy to traktować jako odesłanie do art. 46 ust. 2 lit. c) RODO, który zasadniczo zawiera powtórzenie treści wcześniejszego przepisu³⁰. W związku z tym decyzje wykonawcze przyjęte przez Komisję przed wejściem w życie RODO na mocy art. 26 ust. 4 dyrektywy 95/46 należy interpretować w świetle tego rozporządzenia. Także ważność tych decyzji powinna być w razie potrzeby oceniana na gruncie rzeczonego rozporządzenia.

²⁷ Zobacz pkt 167–186 niniejszej opinii.

²⁸ Zobacz w szczególności wyroki z dnia 10 grudnia 2018 r., Wightman i in. (C-621/18, EU:C:2018:999, pkt 27) oraz z dnia 19 listopada 2019 r., A.K. i in. (Niezależność Izby Dyscyplinarnej Sądu Najwyższego) (sprawy połączone C-585/18, C-624/18 i C-625/18, EU:C:2019:982, pkt 98).

²⁹ Zobacz art. 94 ust. 1 i art. 99 ust. 1 RODO.

³⁰ Należy podkreślić, że zgodnie z art. 46 ust. 5 RODO decyzje przyjęte przez Komisję na mocy art. 26 ust. 4 dyrektywy 95/46 pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylecia.

91. Wniosku tego nie podważa orzecznictwo, w myśl którego zgodność aktu Unii z prawem winna być oceniana w świetle okoliczności faktycznych i prawnych istniejących w dniu, w którym akt ten został wydany. Orzecznictwo to dotyczy bowiem badania ważności aktu Unii w świetle okoliczności faktycznych istotnych w chwili przyjmowania tego aktu³¹ lub w świetle zasad procedury regulującej przyjmowanie tego aktu³². Natomiast Trybunał wielokrotnie badał ważność aktów prawa wtórnego na gruncie materialnoprawnych norm wyższego rzędu, które weszły w życie po przyjęciu tych aktów³³.

92. O ile zatem wskazanie w treści pytań prejudycjalnych aktu prawnego, który nie ma już zastosowania *ratione temporis*, uzasadnia przeformułowanie tych pytań, to nie może ono jednak skutkować ich niedopuszczalnością³⁴. Jak podnieśli DPC i M. Schrems, zawarte w treści pytań prejudycjalnych odesłania do dyrektywy 95/46 można zresztą wyjaśnić biorąc pod uwagę harmonogram proceduralny niniejszej sprawy, ponieważ pytania te zostały przedłożone Trybunałowi przed wejściem w życie RODO.

93. W każdym razie przepisy RODO, które będą omawiane na potrzeby analizy pytań prejudycjalnych – a mianowicie, w szczególności jego art. 45, 46 i 58 – stanowią zasadniczo powtórzenie treści art. 25, 26 i 28 dyrektywy 95/46 (rozbudowując ją i wprowadzając pewne drobne różnice). Jeśli chodzi o czynniki istotne dla oceny ważności decyzji 2010/87, nie dostrzegam żadnego powodu, aby nadawać tym przepisom RODO znaczenie odmienne od znaczenia przepisów dyrektywy 95/46 stanowiących ich odpowiednik³⁵.

2. W przedmiocie tymczasowego charakteru wątpliwości wyrażonych przez DPC

94. Zdaniem rządu niemieckiego rozpatrywany wniosek o wydanie orzeczenia w trybie prejudycjalnym jest niedopuszczalny, ponieważ do skorzystania z drogi prawnej, o której mowa w pkt 65 wyroku Schrems, wymagane jest, aby organ nadzorczy wyrobił sobie ostateczną opinię co do zasadności zarzutów podniesionych przez skarżącego względem ważności rozpatrywanej decyzji. W tym wypadku tak nie jest, ponieważ DPC wyraził wątpliwości co do ważności decyzji 2010/87, która nie została zakwestionowana przez M. Schremsa, w projekcie decyzji, mającym charakter tymczasowy z uwagi na możliwość złożenia przez Facebook Ireland i M. Schremsa uwag dodatkowych.

95. Moim zdaniem tymczasowy charakter wątpliwości wyrażonych przez DPC nie ma wpływu na dopuszczalność odesłania prejudycjalnego. Kryteria dopuszczalności pytania prejudycjalnego powinny bowiem podlegać ocenie z punktu widzenia przedmiotu sporu określonego przez sąd odsyłający³⁶. Nie ma zaś wątpliwości, że spór ten dotyczy ważności decyzji 2010/87. Z brzmienia postanowienia odsyłającego i załączonego do niego wyroku wynika, że sąd ten uznał, iż wyrażone przez DPC wątpliwości – niezależnie od tego, czy mają charakter tymczasowy czy ostateczny – są zasadne, i w konsekwencji zwrócił się do Trybunału z pytaniem o ważność tej decyzji. W tych okolicznościach udzielenie przez Trybunał wyjaśnień w tym przedmiocie niewątpliwie jest istotne dla umożliwienia temu sądowi rozstrzygnięcia zawisłego przed nim sporu.

31 Zobacz w szczególności wyroki z dnia 7 lutego 1979 r., Francja/Komisja (sprawy połączone 15/76 i 16/76, EU:C:1979:29, pkt 7); z dnia 17 maja 2001 r., IECC/Komisja (C-449/98 P, EU:C:2001:275, pkt 87); z dnia 17 października 2013 r., Schaible (C-101/12, EU:C:2013:661, pkt 50).

32 Zobacz w szczególności wyroki z dnia 16 kwietnia 2015 r., Parlament/Rada (C-540/13, EU:C:2015:224, pkt 35); z dnia 16 kwietnia 2015 r., Parlament/Rada (sprawy połączone C-317/13 i C-679/13, EU:C:2015:223, pkt 45); z dnia 22 września 2016 r., Parlament/Rada (sprawy połączone C-14/15 i C-116/15, EU:C:2016:715, pkt 48).

33 W szczególności w wyroku Schrems Trybunał dokonał oceny ważności decyzji w sprawie bezpiecznej przystani w świetle postanowień karty, która została przyjęta później niż ta decyzja. Zobacz również wyroki z dnia 17 marca 2011 r., AJD Tuna (C-221/09, EU:C:2011:153, pkt 48); z dnia 11 czerwca 2015 r., Pfeifer & Langen (C-51/14, EU:C:2015:380, pkt 42).

34 Zobacz w szczególności wyroki z dnia 15 lipca 2010 r., Pannon Gép Centrum (C-368/09, EU:C:2010:441, pkt 30–35); z dnia 10 lutego 2011 r., Andersson (C-30/10, EU:C:2011:66, pkt 20 i 21); z dnia 25 października 2018 r., Roche Lietuva (C-413/17, EU:C:2018:865, pkt 17–20).

35 Zobacz w tym względzie opinię rzecznika generalnego M. Bobeka w sprawie Fashion ID (C-40/17, EU:C:2018:1039, pkt 87).

36 Zobacz pkt 87 niniejszej opinii.

3. W przedmiocie wątpliwości dotyczących ustalenia okoliczności faktycznych

96. Rząd Zjednoczonego Królestwa twierdzi, że opis okoliczności faktycznych przedstawiony przez sąd odsyłający zawiera kilka luk, które wyłączają możliwość uznania pytań prejudycjalnych za dopuszczalne. Sąd ten nie wyjaśnił, czy dane osobowe dotyczące M. Schremsa zostały rzeczywiście przekazane do Stanów Zjednoczonych, a jeżeli tak, to czy były one gromadzone przez organy amerykańskie. Brak jest również pewności co do podstawy prawna ewentualnego przekazywania tych danych, ponieważ postanowienie odsyłające ogranicza się do stwierdzenia, że dane europejskich użytkowników sieci społecznościowej Facebook są przekazywane „w dużej części” na podstawie standardowych klauzul umownych przewidzianych w decyzji 2010/87. W każdym razie nie zostało wykazane, że wskazana jako podstawa spornego przekazywania danych umowa, która została zawarta pomiędzy Facebook Ireland a Facebook Inc., zawiera te właśnie klauzule. Rząd niemiecki kwestionuje dopuszczalność odesłania prejudycjalnego także z tego względu, że sąd odsyłający nie zbadał, czy M. Schrems jednoznacznie wyraził zgodę na przekazanie jego danych, co sprawiłoby, iż miałyby ono należytą podstawę prawną w postaci art. 26 ust. 1 dyrektywy 95/46 [którego treść została zasadniczo powtórzona w art. 49 ust. 1 lit. a) RODO].

97. Argumenty te w żadnym razie nie podważają znaczenia, jakie ma odesłanie prejudycjalne dla sporu zawisłego w postępowaniu głównym. Ponieważ spór ten powstał w związku ze skorzystaniem przez DPC ze środka ochrony prawnej przewidzianego w pkt 65 wyroku Schrems, jego przedmiotem jest właśnie skłonienie sądu krajowego do wystąpienia z odesłaniem prejudycjalnym dotyczącym ważności decyzji 2010/87. W rzeczywistości rząd niemiecki i rząd Zjednoczonego Królestwa kwestionują potrzebę skierowania pytań prejudycjalnych nie dla ustalenia, czy decyzja ta jest ważna, lecz dla umożliwienia DPC wypowiedzenia się *in concreto* co do skargi M. Schremsa.

98. W każdym razie, nawet z punktu widzenia tego postępowania leżącego u podstaw sporu w postępowaniu głównym, pytania prejudycjalne dotyczące ważności decyzji 2010/87 nie wydają mi się pozbawione znaczenia. Sąd odsyłający ustalił bowiem, że Facebook Ireland, po tym, gdy została stwierdzona nieważność decyzji w sprawie bezpiecznej przystani, nadal przekazywała dane osobowe swoich użytkowników do Stanów Zjednoczonych oraz że czyniła to, przynajmniej w części, na podstawie decyzji 2010/87. Ponadto, mimo że ustalenie przez sąd odsyłający wszystkich istotnych okoliczności faktycznych jeszcze przed wykonaniem przezeń uprawnienia wynikającego z art. 267 TFUE może być użyteczne, to wyłącznie do tego sądu należy ocena, na jakim etapie postępowania jest mu potrzebne uzyskanie od Trybunału orzeczenia wydanego w trybie prejudycjalnym³⁷.

99. Mając na względzie powyższe uważam, że wniosek o wydanie orzeczenia w trybie prejudycjalnym jest dopuszczalny.

C. W przedmiocie możliwości zastosowania prawa Unii do przekazywania danych osobowych w celach komercyjnych do państwa trzeciego, w którym mogą one być przetwarzane do celów bezpieczeństwa narodowego (pytanie pierwsze)

100. Poprzez pytanie pierwsze sąd odsyłający zmierza do ustalenia, czy prawo Unii ma zastosowanie do przekazywania danych osobowych w celach komercyjnych przez spółkę mającą siedzibę w państwie członkowskim do spółki mającej siedzibę w państwie trzecim w sytuacji, gdy, po zainicjowaniu tego przekazywania, dane osobowe mogą podlegać przetwarzaniu przez organy publiczne tego państwa trzeciego między innymi do celów ochrony bezpieczeństwa narodowego.

³⁷ Zobacz podobnie wyroki z dnia 1 kwietnia 1982 r., *Holdijk i in.* (141/81–143/81, EU:C:1982:122, pkt 5); z dnia 9 grudnia 2003 r., *Gasser* (C-116/02, EU:C:2003:657, pkt 27).

101. Znaczenie tego pytania dla rozstrzygnięcia sporu w postępowaniu głównym polega na tym, że gdyby takie przekazywanie znajdowało się poza zakresem stosowania prawa Unii, wszystkie podniesione w niniejszej sprawie zastrzeżenia co do ważności decyzji 2010/87 stałyby się bezpodstawne.

102. Jak zauważył sąd odsyłający, przetwarzanie danych osobowych w ramach ochrony bezpieczeństwa narodowego jest wyłączone z zakresu stosowania dyrektywy 95/46 na mocy jej art. 3 ust. 2. Obecnie w art. 2 ust. 2 RODO wyjaśniono, że rozporządzenie to nie ma zastosowania między innymi do przetwarzania danych w ramach działalności nieobjętej zakresem prawa Unii lub przetwarzania przez właściwe organy do celów ochrony bezpieczeństwa publicznego. Przepisy te odzwierciedlają wynikające z art. 4 ust. 2 TUE zastrzeżenie kompetencji dla państw członkowskich w dziedzinie ochrony bezpieczeństwa narodowego.

103. DPC, M. Schrems, Irlandia, rządy niemiecki, austriacki, belgijski, czeski, niderlandzki, polski i portugalski, jak również Parlament i Komisja twierdzą, że przekazywanie danych takie jak to, którego dotyczy skarga M. Schremsa, nie podlega powyższym przepisom, w związku z czym wchodzi w zakres stosowania prawa Unii. Facebook Ireland opowiada się za przeciwnym stanowiskiem. Przychylam się do tego pierwszego poglądu.

104. Należy w tym względzie podkreślić, że przekazywanie danych osobowych z państwa członkowskiego do państwa trzeciego stanowi samo w sobie „przetwarzanie” w rozumieniu art. 4 pkt 2 RODO, dokonywane na terytorium państwa członkowskiego³⁸. Przedmiotem pierwszego pytania prejudycjalnego jest właśnie ustalenie, czy prawo Unii stosuje się *do przetwarzania, które sprowadza się do samego tylko przekazywania danych*. Pytanie to nie dotyczy stosowania prawa Unii do ewentualnego późniejszego przetwarzania (przez organy amerykańskie do celów bezpieczeństwa narodowego) danych, które zostały przekazane do Stanów Zjednoczonych, gdyż takie przetwarzanie z pewnością nie jest objęte terytorialnym zakresem stosowania RODO³⁹.

105. Z tego punktu widzenia, aby ustalić, czy prawo Unii ma zastosowanie do przekazywania danych, którego dotyczy sprawa, należy brać pod uwagę wyłącznie działalność, w której ramy wpisuje się to przekazywanie danych, natomiast nie jest istotny przedmiot ewentualnego dalszego przetwarzania, któremu zostaną poddane dane przekazane przez organy władzy publicznej docelowego państwa trzeciego⁴⁰.

106. Z postanowienia odsyłającego wynika zaś, że przekazywanie danych, o którym mowa w skardze M. Schremsa, stanowi część działalności prowadzonej w celach komercyjnych. Ponadto umożliwienie późniejszego przetwarzania tych danych przez organy amerykańskie do celów bezpieczeństwa narodowego nie jest celem tego przekazywania danych (nawet drugorzędny).

107. Wreszcie, przyjęcie podejścia proponowanego przez Facebook Ireland pozbawiałoby skuteczności przepisy RODO dotyczące przekazywania danych do państw trzecich, ponieważ nigdy nie można wykluczyć, że dane przekazywane w ramach działalności komercyjnej będą później przetwarzane do celów bezpieczeństwa narodowego.

38 Zobacz podobnie wyrok z dnia 30 maja 2006 r., Parlament/Rada i Komisja (sprawy połączone C-317/04 i C-318/04, EU:C:2006:346, zwany dalej „wyrokiem PNR”, pkt 56) oraz wyrok Schrems (pkt 45). Artykuł 4 pkt 2 RODO stanowi zasadniczo powtórzenie definicji „przetwarzania”, która znajdowała się w art. 2 lit. b) dyrektywy 95/46.

39 Zgodnie z art. 3 ust. 1 RODO, rozporządzenie to ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii. Zagadnienie dotyczące stosowania prawa Unii do przetwarzania danych przez służby wywiadu państwa trzeciego poza Unią należy odróżnić od zagadnienia dotyczącego znaczenia zasad i praktyk towarzyszących temu przetwarzaniu w danym państwie trzecim dla ustalenia, czy w państwie tym zapewniony jest odpowiedni stopień ochrony. To ostatnie zagadnienie jest przedmiotem drugiego pytania prejudycjalnego i zostanie przeanalizowane w pkt 201–229 niniejszej opinii.

40 W mojej opinii w sprawie Ministerio Fiscal (C-207/16, EU:C:2018:300, pkt 47) zwróciłem uwagę na wprowadzone rozróżnienie pomiędzy bezpośrednim przetwarzaniem danych osobowych w ramach czynności władczych państwa a przetwarzaniem o charakterze komercyjnym, po którym następuje wykorzystanie przez organy państwa.

108. Proponowana przeze mnie wykładnia znajduje potwierdzenie w treści art. 45 ust. 2 lit. a) RODO. Zgodnie z tym przepisem Komisja, przyjmując decyzję stwierdzającą odpowiedni stopień ochrony, uwzględnia w szczególności ustawodawstwo danego państwa trzeciego *w dziedzinie bezpieczeństwa narodowego*. Można na tej podstawie wyciągnąć wniosek, że możliwość, iż dane będą przetwarzane przez organy docelowego państwa trzeciego do celów ochrony bezpieczeństwa narodowego, nie przesądza o tym, że prawo Unii nie ma zastosowania do przetwarzania polegającego na przekazaniu danych do tego państwa trzeciego.

109. Rozumowanie i wnioski, do jakich doszedł Trybunał w wyroku Schrems, również opierają się na tym założeniu. W wyroku tym Trybunał badał w szczególności ważność decyzji w sprawie bezpiecznej przystani w zakresie, w jakim decyzja ta dotyczyła właśnie przekazywania danych osobowych do Stanów Zjednoczonych, gdzie mogły one być zbierane i przetwarzane do celów ochrony bezpieczeństwa narodowego, na podstawie art. 25 ust. 6 dyrektywy 95/46, w świetle postanowień karty⁴¹.

110. Mając na względzie powyższe rozważania uważam, że prawo Unii ma zastosowanie do dokonywanego w ramach działalności komercyjnej przekazywania danych osobowych z państwa członkowskiego do państwa trzeciego, przy czym bez znaczenia jest okoliczność, że przekazywane dane mogą podlegać przetwarzaniu przez organy publiczne tego państwa trzeciego w celach służących ochronie bezpieczeństwa narodowego rzeczonoego państwa.

D. W przedmiocie stopnia ochrony wymaganego w związku z przekazywaniem danych na podstawie standardowych klauzul umownych (pierwsza część pytania szóstego)

111. Zgodnie z brzmieniem pierwszej części pytania szóstego sąd odsyłający stara się ustalić, jaki stopień ochrony praw podstawowych osób, których dane dotyczą, należy zapewnić, aby te dane osobowe mogły zostać przekazane do państwa trzeciego na podstawie standardowych klauzul umownych przewidzianych w decyzji 2010/87.

112. Sąd ten podkreśla, że w wyroku Schrems Trybunał dokonał takiej wykładni art. 25 ust. 6 dyrektywy 95/46 (którego treść została zasadniczo powtórzona w art. 45 ust. 3 RODO), zgodnie z którą przepis ten umożliwia Komisji przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony wyłącznie wówczas, jeżeli upewni się ona, iż dane państwo trzecie zapewnia *odpowiedni* stopień ochrony, co wymaga ustalenia przez nią, że państwo to zapewnia stopień ochrony podstawowych praw i wolności *merytorycznie równoważny* stopniowi ochrony gwarantowanemu w Unii na mocy tej dyrektywy w związku z kartą⁴².

113. W tym kontekście pierwsza część szóstego pytania prejudycjalnego wymaga od Trybunału ustalenia, czy zastosowanie „standardowych klauzul umownych” przyjmowanych przez Komisję na podstawie art. 26 ust. 4 dyrektywy 95/46 – odpowiadających „standardowym klauzulom ochrony danych”, o których mowa obecnie w art. 46 ust. 2 lit. c) RODO – powinno umożliwić osiągnięcie stopnia ochrony odpowiadającego temu samemu standardowi „merytorycznej równoważności”.

41 Podobnie w opinii 1/15 (Umowa PNR UE–Kanada) z dnia 26 lipca 2017 r. (EU:C:2017:592, zwanej dalej „opinią 1/15”), Trybunał badał, czy projekt zawartej między Kanadą a Unią umowy międzynarodowej dotyczącej danych, które po przekazaniu do Kanady miały być poddawane przetwarzaniu przez organy publiczne do celów ochrony bezpieczeństwa narodowego, jest zgodny z art. 7, 8 i 47 karty.

42 Wyrok Schrems (pkt 73). Trybunał potwierdził ten wniosek w opinii 1/15 (pkt 134).

114. Artykuł 46 ust. 1 RODO stanowi w tym względzie, że w razie braku decyzji stwierdzającej odpowiedni stopień ochrony, administrator może przekazać dane osobowe do państwa trzeciego „wyłącznie, gdy [zapewni] *odpowiednie zabezpieczenia*, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej” (wyróżnienie moje)⁴³. Zgodnie z art. 46 ust. 2 lit. c) RODO zabezpieczenia te mogą wynikać między innymi ze standardowych klauzul ochrony danych opracowanych przez Komisję.

115. Podobnie jak DPC, M. Schrems i Irlandia uważam, że zapewniane przez administratora „odpowiednie zabezpieczenia”, o których mowa w art. 46 ust. 1 RODO, powinny gwarantować, że prawa przysługujące osobom, których dane są przekazywane korzystają (podobnie jak w przypadku przekazywania na podstawie decyzji stwierdzającej odpowiedni stopień ochrony) z poziomu ochrony równoważnego pod względem merytorycznym z tym, który wynika z RODO interpretowanego w świetle karty.

116. Powyższy wniosek wynika z celu, jakiemu służy ten przepis, oraz z aktu prawnego, w którym jest zawarty.

117. Artykuły 45 i 46 RODO mają na celu zapewnienie ciągłości stopnia ochrony danych osobowych gwarantowanego przez to rozporządzenie, w sytuacji gdy dane te są przekazywane poza Unię. Artykuł 44 RODO zatytułowany „Ogólna zasada przekazywania” otwiera bowiem rozdział V dotyczący przekazywania danych osobowych do państw trzecich i stanowi, że wszystkie przepisy tego rozdziału należy stosować z myślą o zapewnieniu, by w sytuacji, gdy dane osobowe są przekazywane do państwa trzeciego, nie został naruszony stopień ochrony osób fizycznych zagwarantowany w RODO⁴⁴. Zasada ta ma na celu uniknięcie sytuacji, w której standardy ochrony wynikające z prawa Unii byłyby obchodzone poprzez przekazanie danych osobowych do państwa trzeciego w celu ich przetwarzania w tym państwie⁴⁵. Mając na uwadze ów cel obojętne jest, czy przekazywanie danych odbywa się na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, czy na podstawie zabezpieczeń zapewnianych przez administratora, w szczególności poprzez klauzule umowne. Wymogi ochrony praw podstawowych gwarantowanych w karcie nie różnią się w zależności od podstawy prawnej, na której opiera się określone przekazywanie danych⁴⁶.

118. Natomiast sposoby zapewnienia ciągłości wysokiego stopnia ochrony różnią się w zależności od podstawy prawnej przekazywania danych.

119. Po pierwsze, przedmiotem decyzji stwierdzającej odpowiedni stopień ochrony jest stwierdzenie, że dane państwo trzecie samodzielnie zapewnia stopień ochrony równoważny pod względem merytorycznym z tym, którego osiągnięcia wymaga prawo Unii. Przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony winno być poprzedzone dokonaniem przez Komisję, w odniesieniu do określonego państwa trzeciego, oceny stopnia ochrony zapewnianego przez prawo i praktyki stosowane w tym państwie trzecim w świetle czynników wymienionych w art. 45 ust. 3 RODO. W takim przypadku dane osobowe mogą być przekazane do tego państwa trzeciego bez konieczności uzyskiwania przez administratora specjalnego zezwolenia.

43 Artykuł 26 ust. 2 dyrektywy 95/46 przewidywał, że państwo członkowskie może zezwolić na przekazywanie takich danych „jeżeli administrator danych zaleci *odpowiednie zabezpieczenia* odnośnie do ochrony prywatności oraz podstawowych praw i wolności osoby oraz odnośnie do wykonywania odpowiednich praw” (wyróżnienie moje). Wyrażenie „odpowiednie zabezpieczenia” zawarte w tym przepisie oraz wyrażenie „odpowiednie zabezpieczenia”, zawarte w art. 46 ust. 1 RODO, mają według mnie tę samą treść [uwaga tłumacza – w j. polskim zarówno w dyrektywie, jak i w rozporządzeniu jest to identyczne wyrażenie].

44 W tym względzie motyw 6 RODO wskazuje, że należy zapewnić „wysoki stopień” ochrony danych osobowych zarówno wewnątrz Unii, jak i w przypadku ich przekazywania poza Unię. Zobacz również motyw 101 RODO.

45 Zobacz wyrok Schrems (pkt 73) i opinię 1/15 (pkt 214).

46 Nie podważa to możliwości przekazywania danych osobowych nawet w przypadku braku odpowiednich zabezpieczeń, na podstawie wyjątków przewidzianych w art. 49 ust. 1 RODO.

120. Po drugie (co zostanie omówione dokładniej w następnej części niniejszej opinii), oferowane przez administratora odpowiednie zabezpieczenia służą zapewnieniu wysokiego stopnia ochrony na wypadek, gdyby zabezpieczenia dostępne w docelowym państwie trzecim były niewystarczające. Chociaż więc w art. 46 ust. 1 RODO przewidziana została możliwość przekazywania danych osobowych do państw trzecich, które nie zapewniają odpowiedniego stopnia ochrony, to przepis ten zezwala na takie przekazywanie wyłącznie wtedy, gdy odpowiednie zabezpieczenia są zapewnione przy pomocy innych środków. Przyjęte przez Komisję standardowe klauzule umowne stanowią w związku z tym ogólny mechanizm mający zastosowanie do przekazywania danych niezależnie od tego, jakie państwo trzecie jest państwem docelowym ani od tego, jaki stopień ochrony jest w nim zapewniany.

E. W przedmiocie ważności decyzji 2010/87 w świetle art. 7, 8 i 47 karty (pytania siódme, ósme i jedenaste)

121. Poprzez pytanie siódme sąd odsyłający zwraca się w istocie do Trybunału o ustalenie, czy decyzja 2010/87 jest nieważna, gdyż nie wiąże organów władzy państw trzecich, do których przekazywane są dane osobowe na podstawie standardowych klauzul umownych przewidzianych w załączniku do tej decyzji, a w szczególności nie stoi ona na przeszkodzie nałożeniu na podmiot odbierający dane wymogu przekazania tych danych do dyspozycji tych organów. Pytanie to poddaje zatem w wątpliwość samą możliwość zapewnienia odpowiedniego stopnia ochrony takich danych przy pomocy mechanizmu o wyłącznie kontraktowym charakterze. Pytanie jedenaste odnosi się ogólnie do ważności decyzji 2010/87 w świetle art. 7, 8 i 47 karty.

122. W ramach pytania ósmego zadaniem Trybunału jest ustalenie, czy organ nadzorczy ma obowiązek skorzystania z uprawnień powierzonych mu na mocy art. 58 ust. 2 lit. f) i j) RODO i zawiesić przekazywanie danych do państwa trzeciego oparte na standardowych klauzulach umownych przewidzianych w decyzji 2010/87, gdy uzna, że na podmiot odbierający dane podlega w tym państwie nałożone zostały obowiązki, które uniemożliwiają mu przestrzeganie tych klauzul i które skutkują brakiem zapewnienia odpowiedniej ochrony przekazanych danych osobowych. Ponieważ, moim zdaniem, odpowiedź na to pytanie ma wpływ na ważność decyzji 2010/87⁴⁷, przeanalizuję je łącznie z pytaniami siódmym i jedenastym.

123. Treść art. 46 ust. 1 RODO, zgodnie z którym „[w] razie braku decyzji na mocy art. 45 ust. 3 administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego [...] wyłącznie gdy zapewnią odpowiednie zabezpieczenia” (wyróżnienie moje), stanowi wyraz logiki leżącej u podstaw mechanizmów kontraktowych, takich jak ten przewidziany w decyzji 2010/87. Jak podkreślono w motywach 108 i 114 RODO, mechanizmy te mają na celu umożliwienie przekazywania danych do państw trzecich, w stosunku do których Komisja nie przyjęła decyzji stwierdzającej odpowiedni stopień ochrony, w taki sposób, że ewentualne braki ochrony zapewnianej w porządku prawnym tego państwa trzeciego są *rekompensowane* poprzez zabezpieczenia, które podmiot przekazujący dane i podmiot odbierający zobowiązują się zapewnić na podstawie umowy.

124. Skoro więc celem zabezpieczeń o charakterze kontraktowym jest właśnie uzupełnienie możliwych braków w ochronie zapewnianej przez docelowe państwa trzecie (jakikolwiek by one nie były), ważność decyzji, w której Komisja stwierdza, że pewne standardowe klauzule w odpowiedni sposób uzupełniają te braki, nie może zależeć od stopnia ochrony, jaki zapewniają poszczególne państwa trzecie, do których mogłyby być przekazane dane osobowe. Ważność takiej decyzji zależy wyłącznie od skuteczności zabezpieczeń ustanowionych poprzez te klauzule w celu zrekompensowania ewentualnych braków ochrony w docelowym państwie trzecim. Skuteczność tych zabezpieczeń należy oceniać uwzględniając również ochronę, jaką dają uprawnienia organów nadzorczych, wynikające z art. 58 ust. 2 RODO.

⁴⁷ Zobacz pkt 128 niniejszej opinii.

125. W związku z tym, jak zauważyli zasadniczo DPC, M. Schrems, BSA, Irlandia, rządy austriacki, francuski, polski i portugalski oraz Komisja, zabezpieczenia zawarte w standardowych klauzulach umownych mogą zostać osłabione a nawet unicestwione w sytuacji, gdy prawo docelowego państwa trzeciego nakłada na podmiot odbierający dane obowiązki, które stoją w sprzeczności z wymogami wynikającymi z tych klauzul. Zatem kontekst prawny dominujący w docelowym państwie trzecim może, w zależności od konkretnych okoliczności, w jakich odbywa się przekazywanie danych⁴⁸, uniemożliwić wypełnienie zobowiązań wynikających z tych klauzul.

126. W związku z tym, jak podkreślili M. Schrems i Komisja, istotą kontraktowego mechanizmu przewidzianego w art. 46 ust. 2 lit. c) RODO jest nałożenie odpowiedzialności na podmiot przekazujący dane oraz, pomocniczo, na organy nadzorcze. Wobec tego, administrator lub, w razie jego beczynności, organ nadzorczy powinien badać *indywidualnie* dla każdego konkretnego przypadku przekazywania danych, czy prawo docelowego państwa trzeciego stoi na przeszkodzie wykonaniu zobowiązań wynikających ze standardowych klauzul umownych, uniemożliwiając odpowiednią ochronę przekazanych danych, efektem należałoby zakazać przekazywania lub zawiesić je.

127. Mając na względzie powyższe uwagi stoję na stanowisku, że okoliczność, iż decyzja 2010/87 i zawarte w niej standardowe klauzule umowne nie są wiążące dla organów docelowego państwa trzeciego, sama w sobie nie skutkuje nieważnością tej decyzji. Zgodność decyzji 2010/87 z art. 7, 8 i 47 karty zależy moim zdaniem od tego, czy istnieją dostatecznie skuteczne mechanizmy pozwalające zapewnić, że przekazywanie danych w oparciu o standardowe klauzule umowne zostanie zawieszone lub zakazane w przypadku naruszenia tych klauzul lub braku możliwości ich wypełnienia.

128. Artykuł 46 ust. 1 RODO stanowi w tym względzie, że przekazywanie danych w oparciu o odpowiednie zabezpieczenia może nastąpić wyłącznie „pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą, i skuteczne środki ochrony prawnej”. Należy zweryfikować, czy zabezpieczenia przewidziane w klauzulach znajdujących się w załączniku do decyzji 2010/87, uzupełnione o uprawnienia przysługujące organom nadzorczym, umożliwiają zapewnienie spełnienia tego warunku. Według mnie jest tak wyłącznie, jeśli istnieje *obowiązek* – ciążyący na administratorach (część 1) oraz, w przypadku ich beczynności, na organach nadzorczych (część 2) – wprowadzenia zawieszenia lub zakazu przekazywania danych w sytuacji, gdy, ze względu na konflikt między zobowiązaniami wynikającymi ze standardowych klauzul a tymi, jakie nakłada prawo docelowego państwa trzeciego, klauzule te nie mogą być przestrzegane.

1. W przedmiocie obowiązków ciążących na administratorach

129. Po pierwsze, standardowe klauzule umowne zawarte w załączniku do decyzji 2010/87 ustanawiają wymóg, zgodnie z którym w przypadku sprzeczności między przewidzianymi w nich obowiązkami a przepisami obowiązującymi w docelowym państwie trzecim, klauzule te nie mogą stanowić podstawy przekazywania danych do tego państwa, a jeżeli przekazywanie na podstawie tych klauzul zostało już zainicjowane, o tej sprzeczności należy poinformować podmiot przekazujący dane, który może zawiesić przekazywanie.

⁴⁸ Wyobraźmy sobie na przykład, że państwo trzecie nakłada na dostawców usług telekomunikacyjnych obowiązek udzielenia organom publicznym dostępu do przekazywanych danych bez jakichkolwiek ograniczeń ani zabezpieczeń. O ile tacy dostawcy nie mają, w związku z powyższym, możliwości przestrzegania standardowych klauzul umownych, to przedsiębiorstwa, które nie podlegają temu obowiązkowi mogłyby wywiązywać się z nich bez przeszkód.

130. I tak, zgodnie z klauzulą 5 lit. a) podmiot odbierający dane zobowiązuje się przetwarzać dane osobowe wyłącznie w imieniu podmiotu przekazującego dane i zgodnie z jego instrukcjami oraz ze standardowymi klauzulami umownymi. Jeżeli podmiot odbierający dane z jakichkolwiek powodów nie może zapewnić zgodności z tymi klauzulami, zgadza się on na natychmiastowe poinformowanie podmiotu przekazującego dane o niemożności spełnienia tego warunku, a podmiot przekazujący dane jest w takim przypadku uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy⁴⁹.

131. Przypis 5 odnoszący się do klauzuli 5 zawiera wyjaśnienie, zgodnie z którym do naruszenia standardowych klauzul nie dochodzi w sytuacji, gdy podmiot odbierający dane działa wykonując wymogi przepisów krajowych o charakterze bezwzględnie obowiązującym, mających do niego zastosowanie w państwie trzecim, o ile wymogi te nie wykraczają poza to, co jest niezbędne w demokratycznym społeczeństwie w celu ochrony wartości wyszczególnionych w art. 13 ust. 1 dyrektywy 95/46 (którego treść została zasadniczo powtórzona w art. 23 ust. 1 RODO), między innymi bezpieczeństwa publicznego i narodowego. Z kolei niewykonanie tych klauzul z uwagi na konieczność spełnienia sprzecznego z nimi obowiązku wynikającego z prawa docelowego państwa trzeciego, który to obowiązek jest nieproporcjonalny w stosunku do ochrony prawnie uzasadnionego interesu uznanego przez Unię, jest traktowane jako naruszenie tych klauzul.

132. Podobnie jak twierdzą M. Schrems i Komisja uważam, że klauzuli 5 lit. a) nie można interpretować w ten sposób, że zawieszenie przekazywania danych lub rozwiązanie umowy jest jedynie fakultatywne w przypadku, gdy podmiot odbierający dane nie jest w stanie przestrzegać tych standardowych klauzul. Mimo, że w klauzuli tej jest mowa wyłącznie o prawie, jakie przysługuje w tym względzie podmiotowi przekazującemu dane, jej treść należy rozpatrywać uwzględniając kontekst umowny, w który jest włączona. Okoliczność, że podmiot przekazujący dane, *w ramach dwustronnych relacji łączących go z podmiotem odbierającym dane*, jest uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy w sytuacji, gdy ten ostatni nie jest w stanie wywiązać się z obowiązków wynikających ze standardowych klauzul, nie zmienia faktu, że na podmiocie przekazującym dane spoczywa obowiązek wykonania tego uprawnienia ze względu na *wynikające z RODO wymogi ochrony praw osób, których dane dotyczą*. Jakakolwiek odmienna wykładnia skutkowałaby nieważnością decyzji 2010/87, skoro zawarte w niej standardowe klauzule umowne nie umożliwiałyby zapewnienia „odpowiednich zabezpieczeń” przekazywanych danych, wymaganych przez art. 46 ust. 1 RODO interpretowany w świetle postanowień karty⁵⁰.

133. Ponadto, zgodnie z brzmieniem klauzuli 5 lit. b) podmiot odbierający dane potwierdza, że nie ma powodu, by sądzić, że prawodawstwo mające do niego zastosowanie uniemożliwia mu wypełnianie instrukcji otrzymanych od podmiotu przekazującego dane i jego obowiązków wynikających z umowy. W przypadku zmiany prawodawstwa, która może mieć istotne negatywne skutki dla gwarancji i obowiązków określonych w standardowych klauzulach, podmiot odbierający dane zawiadomi o tym jak najszybciej podmiot przekazujący dane, który w takim przypadku jest uprawniony do zawieszenia przekazywania danych lub rozwiązania umowy. Zgodnie z klauzulą 4 lit. g) podmiot przekazujący dane obowiązany jest przesłać właściwemu organowi nadzorcemu zawiadomienie otrzymane od podmiotu odbierającego dane, w przypadku gdy zdecyduje się kontynuować przekazywanie danych.

49 Chciałbym poza tym zauważyć, że klauzula 5 lit. d) ppkt i) zwalnia podmiot odbierający dane z obowiązku informowania podmiotu przekazującego dane o prawnie wiążących wnioskach o ujawnienie danych osobowych ze strony organów ścigania państwa trzeciego, gdy prawo tego państwa sprzeciwia się przekazaniu takiej informacji. W takich sytuacjach podmiot przekazujący dane nie będzie miał możliwości zawieszenia przekazywania danych, jeżeli ich ujawnienie, o którym podmiot ten nie wie, narusza standardowe klauzule. Jednakże podmiot odbierający dane pozostaje w takiej sytuacji zobowiązany na mocy klauzuli 5 lit. a) do poinformowania podmiotu przekazującego dane o tym, że w jego ocenie przepisy tego państwa trzeciego uniemożliwiają mu wykonywanie jego zobowiązań wynikających ze standardowych klauzul zawartych w umowie.

50 Z orzecznictwa wynika, że przepisy aktu wykonawczego należy interpretować zgodnie z przepisami aktu podstawowego, w którym ustawodawca zawarł upoważnienie do przyjęcia aktu wykonawczego [zob. podobnie w szczególności wyroki z dnia 26 lipca 2017 r., Republika Czeska/Komisja (C-696/15 P, EU:C:2017:595, pkt 51); z dnia 17 maja 2018 r., Evonik Degussa (C-229/17, EU:C:2018:323, pkt 29); z dnia 20 czerwca 2019 r., ExxonMobil Production Deutschland (C-682/17, EU:C:2019:518, pkt 112)]. Poza tym, akt prawny Unii powinien być interpretowany – tak dalece jak to możliwe – w sposób, który nie podważa jego ważności, i w zgodzie z całością prawa pierwotnego, w tym w szczególności z postanowieniami karty [zob. m.in. wyrok z dnia 14 maja 2019 r., M i in. (Cofnięcie statusu uchodźcy) (sprawy połączone C-391/16, C-77/17 i C-78/17, EU:C:2019:403, pkt 77 i przytoczone tam orzecznictwo)].

134. Uważam, że należy w tym miejscu poczynić pewne wyjaśnienia odnośnie do przedmiotu badania, jakie powinny przeprowadzić strony umowy w celu ustalenia (w związku z przypisem do klauzuli 5), czy obowiązki nakładane przez państwo trzecie na podmiot odbierający dane skutkują naruszeniem standardowych klauzul, a tym samym uniemożliwiają „odpowiednie zabezpieczenie” przekazywanych danych. Zasadniczo problematyka ta została poruszona w ramach drugiej części szóstego pytania prejudycjalnego.

135. Badanie takie wymaga moim zdaniem uwzględnienia całokształtu okoliczności charakteryzujących każdy przypadek przekazywania danych, przy czym do okoliczności takich można zaliczyć rodzaj danych i ich ewentualny wrażliwy charakter, mechanizmy wdrożone przez podmiot przekazujący dane lub podmiot odbierający dane dla zapewnienia ich bezpieczeństwa⁵¹, charakter i cel przetwarzania, jakiemu zostaną poddane dane przez organy publiczne państwa trzeciego, zasady tego przetwarzania oraz ograniczenia i zabezpieczenia, jakie zapewnia to państwo trzecie. Czynniki charakteryzujące przetwarzanie danych przez organy publiczne oraz zabezpieczenia mające zastosowanie w porządku prawnym tego państwa trzeciego moim zdaniem mogą pokrywać się z tymi, o których mowa w art. 45 ust. 2 RODO.

136. Po drugie, w standardowych klauzulach umownych sformułowanych w załączniku do decyzji 2010/87 przyznano osobom, których dane dotyczą, egzekwowalne prawa i środki ochrony prawnej, którymi może ona się posłużyć przeciwko podmiotowi przekazującemu dane oraz, pomocniczo, przeciwko podmiotowi odbierającemu dane.

137. I tak, klauzula 3 zatytułowana „Klauzula na rzecz osoby trzeciej”, w ust. 1 ustanawia na rzecz osoby, której dotyczą dane, środek ochrony prawnej przeciwko podmiotowi przekazującemu dane, między innymi w przypadku naruszenia klauzuli 5 lit. a) lub b). Zgodnie z klauzulą 3 ust. 2, w przypadkach, w których podmiot przekazujący dane przestał istnieć faktycznie lub formalnie, osoba, której dane dotyczą może żądać wykonania tej klauzuli przez podmiot odbierający dane.

138. Klauzula 6 ust. 1 przyznaje każdej osobie, której dotyczą dane i która poniosła szkodę w wyniku naruszenia obowiązków wskazanych w klauzuli 3, prawo do uzyskania odszkodowania za poniesioną szkodę od podmiotu przekazującego dane. Zgodnie z klauzulą 7 ust. 1 podmiot odbierający dane zgadza się na to, że jeżeli osoba, której dotyczą dane, powołuje się wobec niego na prawa osoby trzeciej, na rzecz której zawarto umowę lub występuje o odszkodowanie za szkody, podmiot ten przyjmie decyzję osoby, której dane dotyczą, o przekazaniu sporu do mediacji prowadzonej przez niezależną osobę lub, w stosownych przypadkach, organ nadzorczy bądź przekazaniu sporu do sądów w państwie członkowskim, w którym prowadzi działalność gospodarczą podmiot przekazujący dane.

139. Osoby, których dane dotyczą, oprócz korzystania ze środków ochrony prawnej przysługujących im na podstawie standardowych klauzul umownych przewidzianych w załączniku do decyzji 2010/87, mogą, gdy uznają, że doszło do naruszenia tych klauzul, zwrócić się do organów nadzorczych, aby te wykonały uprawnienia naprawcze na podstawie art. 58 ust. 2 RODO, do którego odsyła art. 4 decyzji 2010/87⁵².

51 W tym względzie motyw 109 RODO zachęca podmiot przekazujący dane i podmiot odbierający je do stosowania (w szczególności na podstawie umowy) dodatkowych zabezpieczeń uzupełniających standardowe klauzule ochrony danych.

52 Mimo że art. 4 ust. 1 decyzji 2010/87 odsyła do art. 28 ust. 3 dyrektywy 95/46, przypominam, że zgodnie z art. 94 ust. 2 RODO odesłania do tej dyrektywy należy traktować jako odesłania do odpowiednich przepisów RODO.

2. W przedmiocie obowiązków spoczywających na organach nadzorczych

140. Następujące powody skłaniają mnie do uznania (za M. Schremsem, Irlandią, rządami niemieckim, austriackim, belgijskim, niderlandzkim i portugalskim oraz EROD), że art. 58 ust. 2 RODO nakłada na organy nadzorcze – gdy uznają one po przeprowadzeniu starannego badania, że dane przekazywane do państwa trzeciego nie są objęte odpowiednią ochroną z powodu nieprzestrzegania uzgodnionych klauzul umownych – obowiązek podjęcia odpowiednich środków w celu usunięcia tej niezgodności z prawem, nakazując w razie potrzeby zawieszenie przekazywania danych.

141. Po pierwsze, zwracam uwagę, że, wbrew temu, co twierdzi DPC, żaden przepis decyzji 2010/87 nie ogranicza do wyjątkowych przypadków uprawnienia przysługującego organom nadzorczym na podstawie art. 58 ust. 2 lit. f) i j) RODO do „wprowadzania czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania” oraz „nakazania zawieszenia przepływu danych do odbiorcy w państwie trzecim”.

142. Co prawda art. 4 ust. 1 decyzji 2010/87 w pierwotnej wersji ograniczał wykonywanie przez organy nadzorcze ich uprawnień w zakresie zawieszania lub zakazywania transgranicznego przepływu danych do pewnych przypadków, w których ustalono, że przekazanie na podstawie umowy może mieć istotne negatywne skutki w odniesieniu do gwarancji mających zapewniających odpowiednią ochronę osób, których dane dotyczą. Jednakże art. 4 tej decyzji, zmieniony przez Komisję w 2016 r. w celu dostosowania jej do wyroku Schrems⁵³, aktualnie jedynie odsyła do tych uprawnień, w żaden sposób ich nie ograniczając. W każdym razie decyzja wykonawcza Komisji, jaką jest decyzja 2010/87, nie może skutecznie ograniczyć uprawnień przyznanych organom nadzorczym na mocy samego RODO⁵⁴.

143. Wniosku tego nie podważa motyw 11 decyzji 2010/87, zgodnie z którym organy nadzorcze mogą korzystać z uprawnień do zawieszenia i zakazania przekazywania danych wyłącznie „w wyjątkowych przypadkach”. Ten motyw, obecny już w pierwotnej wersji decyzji, odnosił się do dawnego art. 4 ust. 1 omawianej decyzji, który ograniczał uprawnienia organów nadzorczych. Zmieniając decyzję 2010/87 poprzez decyzję 2016/2297, Komisja nie usunęła ani nie zmieniła tego motywu, tak aby dostosować jego treść do brzmienia nowego art. 4. Jednakże motyw 5 decyzji 2016/2297 potwierdził przysługujące organom nadzorczym uprawnienie do zawieszenia lub zakazania przekazywania danych, gdy przekazywanie takie zostanie przez nie uznane za sprzeczne z prawem Unii, w szczególności z powodu nieprzestrzegania przez podmiot odbierający dane standardowych klauzul umownych. W związku z tym należy uznać motyw 11 decyzji 2010/87 za nieaktualny, jako że jest on obecnie sprzeczny zarówno z brzmieniem jak i z celem prawnie wiążącego przepisu⁵⁵.

144. Po drugie, także wbrew temu, co twierdzi DPC, wykonywanie uprawnień do zawieszania i zakazywania przekazywania danych ustanowionych w przepisach art. 58 ust. 2 lit. f) i j) RODO, do których odsyła art. 4 decyzji 2010/87, nie stanowi też wyłącznie fakultatywnego uprawnienia pozostawionego uznaniu organów nadzorczych. Moim zdaniem wniosek ten wynika z wykładni art. 58 ust. 2 RODO w świetle innych przepisów tego rozporządzenia i karty oraz z ogólnej systematyki i celów decyzji 2010/87.

53 Zobacz motywy 6 i 7 decyzji 2016/2297. W pkt 101–104 wyroku Schrems, Trybunał orzekł, że przepis decyzji w sprawie bezpiecznej przystani, który ograniczał do „wyjątkowych przypadków” uprawnienia przyznane organom nadzorczym na mocy art. 28 dyrektywy 95/46, jest nieważny, ponieważ Komisja nie miała kompetencji, aby ograniczać te uprawnienia.

54 Zobacz wyrok Schrems (pkt 103).

55 W każdym razie preambuła aktu prawnego Unii nie jest prawnie wiążąca i nie można powołać się na nią w celu tworzenia odstępstw od przepisów zawartych w tym akcie. Zobacz wyroki z dnia 19 listopada 1998 r., Nilsson i in. (C-162/97, EU:C:1998:554, pkt 54); z dnia 12 maja 2005 r., Meta Fackler (C-444/03, EU:C:2005:288, pkt 25); z dnia 10 stycznia 2006 r., IATA i ELFAA (C-344/04, EU:C:2006:10, pkt 76).

145. Artykuł 58 ust. 2 RODO należy w szczególności interpretować w świetle art. 8 ust. 3 karty i art. 16 ust. 2 TFUE. Zgodnie z tymi postanowieniami przestrzeganie wymogów wynikających z prawa podstawowego (jakim jest prawo do ochrony danych osobowych) podlega kontroli niezależnych organów. To zadanie w zakresie sprawowania kontroli przestrzegania wymogów dotyczących ochrony danych osobowych, wskazane również w art. 57 ust. 1 lit. a) RODO, wymaga nałożenia na organy nadzorcze obowiązku działania w sposób, który zapewni należyte stosowanie tego rozporządzenia.

146. W związku z tym organ nadzorczy obowiązany jest rozpatrzyć z wszelką wymaganą starannością skargę wniesioną przez osobę, która zarzuca, że jej dane zostały przekazane do państwa trzeciego z naruszeniem standardowych klauzul umownych mających zastosowanie do przekazywania tych danych⁵⁶. Artykuł 58 ust. 1 RODO przyznaje w tym celu organom nadzorczym szerokie uprawnienia dochodzeniowe⁵⁷.

147. Właściwy organ nadzorczy ma również obowiązek odpowiedniego reagowania na stwierdzone w wyniku przeprowadzonego dochodzenia ewentualne naruszenia praw osoby, której dane dotyczą. Organ nadzorczy dysponuje w tym względzie, na mocy art. 58 ust. 2 RODO, szeroką gamą środków – związanych z wykonywaniem różnorodnych uprawnień naprawczych wyszczególnionych w tym przepisie – służących do wykonywania powierzonego mu zadania⁵⁸.

148. Mimo że wybór najbardziej skutecznego środka zależy od uznania właściwego organu nadzorczego przy uwzględnieniu wszystkich okoliczności rozpatrywanego przekazywania danych, organ ten obowiązany jest wywiązać się w pełni z powierzonego mu zadania w zakresie nadzoru. W razie potrzeby organ ten musi zawiesić przekazywanie danych, jeżeli stwierdzi, że standardowe klauzule umowne nie są przestrzegane i że nie można zapewnić odpowiedniej ochrony przekazywanych danych przy pomocy innych środków, a sam podmiot przekazujący dane nie wstrzymał ich przekazywania.

149. Za przyjęciem takiej wykładni przemawia art. 58 ust. 4 RODO, który stanowi, że wykonywanie uprawnień powierzonych organowi nadzorczemu na mocy tego artykułu podlega odpowiednim zabezpieczeniom, w tym prawu do skutecznego środka ochrony prawnej przed sądem zgodnie z art. 47 karty. Ponadto art. 78 ust. 1 i 2 RODO przyznaje każdej osobie prawo do skutecznego środka ochrony prawnej przed sądem przeciwko dotyczącej jej, prawnie wiążącej decyzji organu nadzorczego lub w sytuacji, gdy organ ten zwleka z rozpatrzeniem jej skargi⁵⁹.

150. Jak twierdzą w istocie M. Schrems, BSA, Irlandia, rządy polski i Zjednoczonego Królestwa oraz Komisja, z przepisów tych wynika, że decyzja, w której organ nadzorczy, rozpatrując wniosek osoby wskazującej na ryzyko, iż dotyczące jej dane są przetwarzane w państwie trzecim z naruszeniem jej praw podstawowych, nie wprowadza zakazu lub nie zawiesza przekazywania danych do tego państwa trzeciego, może być zaskarżona do sądu. Uznanie istnienia prawa do środka ochrony prawnej przed sądem zakłada istnienie ograniczonej swobody administracyjnej, a nie – mającego wyłącznie uznaniowy charakter uprawnienia organów nadzorczych. Ponadto M. Schrems i Komisja słusznie

⁵⁶ Zobacz w drodze analogii wyrok Schrems (pkt 63).

⁵⁷ Chciałbym dodać, że zgodnie z klauzulą 8 ust. 2 zawartą w załączniku do decyzji 2010/87 strony umowy uzgadniają, że organ nadzorczy ma prawo do przeprowadzania kontroli podmiotu odbierającego dane na tych samych warunkach, jakie zgodnie z obowiązującymi przepisami, miałyby zastosowanie do kontroli podmiotu przekazującego dane.

⁵⁸ Zobacz podobnie wyrok Schrems (pkt 43).

⁵⁹ W myśl motywu 141 RODO każda osoba powinna mieć prawo do skutecznego środka ochrony prawnej przed sądem, zgodnie z art. 47 karty w sytuacji, gdy organ nadzorczy „nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby”. Zobacz również motywy 129 i 143 RODO.

podkreślili, że wykonywanie skutecznej kontroli sądowej wymaga, aby organ, od którego pochodzi kwestionowany akt, odpowiednio go uzasadnił⁶⁰. Moim zdaniem ten obowiązek uzasadnienia rozciąga się na dokonywany przez organy nadzorcze wybór tego czy innego uprawnienia przyznanego im na podstawie art. 58 ust. 2 RODO.

151. Jednakże należy jeszcze odpowiedzieć na argumenty DPC, który twierdzi, że nawet gdyby organy nadzorcze miały obowiązek zawiesić przekazywanie danych lub zakazać go w sytuacji, gdy wymaga tego ochrona praw osoby, której te dane dotyczą, nie gwarantowałyby to bynajmniej ważności decyzji 2010/87.

152. Po pierwsze, DPC uważa, że taki obowiązek zawieszenia lub zakazania przekazywania danych nie jest środkiem zaradczym na problemy systemowe związane z brakiem odpowiednich zabezpieczeń w państwie trzecim takim jak Stany Zjednoczone. Uprawnienia organów kontrolnych mogą bowiem być wykonywane wyłącznie w sposób zindywidualizowany, w odniesieniu do poszczególnych przypadków, tymczasem luki, które cechują prawo amerykańskie, mają charakter globalny i strukturalny. Powoduje to powstanie ryzyka, że poszczególne organy nadzorcze będą przyjmowały rozbieżne decyzje dotyczące porównywalnych przypadków przekazywania danych.

153. Co się tyczy tej kwestii, nie mogę lekceważyć praktycznych trudności związanych z wyborem rozwiązania legislacyjnego, jakie należy zastosować w celu nałożenia na organy nadzorcze odpowiedzialności za nadzór nad przestrzeganiem praw podstawowych osób, których dane dotyczą, w ramach poszczególnych przypadków przekazywania tych danych czy też ich przepływu do danego odbiorcy. Nie wydaje mi się jednak, aby trudności te skutkowały nieważnością decyzji 2010/87.

154. Uważam bowiem, że prawo Unii nie wymaga wprowadzenia globalnego i prewencyjnego rozwiązania dla wszystkich przypadków przekazywania danych do określonego państwa trzeciego, z którymi mogą wiązać się te same ryzyka naruszenia praw podstawowych.

155. Co więcej, ryzyko fragmentacji stanowisk przyjmowanych przez różne organy nadzorcze jest wpisane w zamierzoną przez prawodawcę strukturę zdecentralizowanego nadzoru⁶¹. Ponadto, jak podkreślił rząd niemiecki, rozdział VII RODO zatytułowany „Współpraca i spójność” ustanawia mechanizmy służące unikaniu tego ryzyka. Artykuł 60 tego rozporządzenia ustanawia, na wypadek transgranicznego przetwarzania danych, procedurę współpracy między zainteresowanymi organami nadzorczymi a organem nadzorczym jednostki organizacyjnej administratora zwanym „wiodącym organem nadzorczym”⁶². W przypadku sprzecznych opinii, spór jest rozstrzygany przez EROD⁶³. Ta ostatnia jest również właściwa do wydawania, na wniosek organu nadzorczego, opinii w przedmiocie zagadnień mających znaczenie dla więcej niż jednego państwa członkowskiego⁶⁴.

156. Po drugie, DPC podnosi, że decyzja 2010/87 jest nieważna w świetle art. 47 karty, ponieważ organy nadzorcze mogą zapewniać ochronę praw osób, których dane dotyczą, wyłącznie na przyszłość, nie oferując rozwiązań osobom, których dane zostały już przekazane. DPC zwraca w szczególności uwagę, że art. 58 ust. 2 RODO nie przewiduje, w odniesieniu do danych zbieranych przez organy publiczne państwa trzeciego, prawa dostępu, prawa do sprostowania i usunięcia, ani możliwości dochodzenia roszczeń odszkodowawczych z tytułu szkód poniesionych przez osoby, których dane dotyczą.

60 Zobacz między innymi wyroki z dnia 28 lipca 2011 r., Samba Diouf (C69/10, EU:C:2011:524, pkt 57); z dnia 17 listopada 2011 r., Gaydarov (C-430/10, EU:C:2011:749, pkt 41).

61 Zobacz na ten temat wyrok z dnia 5 czerwca 2018 r., Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, pkt 69–73).

62 Zobacz art. 56 ust. 1 RODO. Zgodnie z art. 61 tego rozporządzenia organy nadzorcze obowiązane są świadczyć sobie wzajemną pomoc. Artykuł 62 rzeczonoego rozporządzenia upoważnia te organy do prowadzenia wspólnych operacji.

63 Zobacz art. 65 RODO.

64 Zobacz art. 64 ust. 2 RODO.

157. Jeśli chodzi o zarzucany brak prawa dostępu, prawa do sprostowania i usunięcia zebranych danych, należy stwierdzić, że, w sytuacji, gdy w docelowym państwie trzecim nie istnieje żaden skuteczny środek ochrony prawnej, przewidziane w Unii środki ochrony prawnej przeciwko administratorowi nie dają możliwości uzyskania od organów publicznych tego państwa trzeciego dostępu do tych danych lub ich sprostowania czy usunięcia.

158. Moim zdaniem zastrzeżenie to nie uzasadnia jednak niezgodności decyzji 2010/87 z art. 47 karty. Ważność tej decyzji nie zależy bowiem od stopnia ochrony istniejącego w każdym państwie trzecim, do którego dane mogłyby być przekazywane na podstawie zawartych w niej standardowych klauzul umownych. Jeżeli prawo docelowego państwa trzeciego uniemożliwia podmiotowi odbierającemu dane przestrzeganie tych klauzul, ustanawiając wymóg udzielenia dostępu do danych organom publicznym bez zapewnienia możliwości skorzystania z odpowiednich środków ochrony prawnej i jeżeli podmiot przekazujący dane nie zawiesił przekazywania na podstawie klauzuli 5 lit. a) lub b) załącznika do decyzji 2010/87, do organów nadzorczych należy skorzystanie z uprawnień naprawczych.

159. Poza, tym, jak podkreślił M. Schrems, osobom, których prawa zostały naruszone, przysługuje obecnie na podstawie art. 82 RODO roszczenie o naprawienie szkody majątkowej lub niemajątkowej poniesionej w wyniku naruszenia tego rozporządzenia, które może zostać względem administratora lub podmiotu przetwarzającego⁶⁵.

160. Jak wynika z powyższych rozważań, w wyniku przeprowadzonej przeze mnie analizy nie została ujawniona żadna okoliczność, która mogłaby wpływać na ważność decyzji 2010/87 w świetle art. 7, 8 i 47 karty.

F. W przedmiocie braku potrzeby udzielania odpowiedzi na pozostałe pytania prejudycjalne i badania ważności decyzji w sprawie Tarczy Prywatności

161. W tej części przedstawię powody (związane głównie z ograniczeniem przedmiotu sporu w postępowaniu głównym do kwestii ważności decyzji 2010/87), dla których uważam, że nie ma potrzeby udzielania odpowiedzi na pytania od drugiego do piątego oraz na pytania dziewiąte i dziesiąte, ani orzekania co do ważności decyzji w sprawie Tarczy Prywatności.

162. Drugie pytanie prejudycjalne dotyczy wskazania standardów ochrony, jakich powinno przestrzegać państwo trzecie, aby dane mogły być do niego przekazywane zgodnie z prawem na podstawie standardowych klauzul umownych w sytuacji, gdy dane te, po ich przekazaniu, mogą być przetwarzane przez organy władz tego państwa do celów bezpieczeństwa narodowego. Trzecie z przedłożonych Trybunałowi pytań dotyczy ustalenia elementów charakteryzujących system ochrony obowiązujący w docelowym państwie trzecim, jakie należy uwzględniać badając, czy spełnia on te standardy.

163. Poprzez pytania czwarte, piąte i dziesiąte sąd odsyłający stara się w istocie ustalić, czy, uwzględniając ustalone przezeń okoliczności dotyczące prawa Stanów Zjednoczonych, w państwie tym przewidziane są odpowiednie zabezpieczenia przed ingerencją amerykańskich organów wywiadu w korzystanie z praw podstawowych, jakimi są prawo do poszanowania życia prywatnego, do ochrony danych osobowych oraz do skutecznej ochrony sądowej.

⁶⁵ Artykuł 83 ust. 5 lit. c) RODO przewiduje również administracyjne kary pieniężne w przypadku naruszenia przez administratora art. 44–49 tego rozporządzenia.

164. Dziewiąte pytanie prejudycjalne dotyczy znaczenia, jakie ma poczynione przez Komisję w decyzji w sprawie Tarczy Prywatności ustalenie, zgodnie z którym Stany Zjednoczone oferują odpowiedni stopień ochrony praw podstawowych osób, których dane dotyczą, przed taką ingerencją, dla przeprowadzanej przez organ nadzorczy weryfikacji mającej na celu ustalenie, czy przekazywaniu danych do Stanów Zjednoczonych w oparciu o standardowe klauzule umowne przewidziane w decyzji 2010/87 towarzyszą odpowiednie zabezpieczenia.

165. Sama kwestia ważności decyzji w sprawie Tarczy Prywatności nie została wyraźnie poruszona przez sąd odsyłający – mimo że, jak wyjaśniam poniżej⁶⁶ – pytania prejudycjalne czwarte, piąte i dziesiąte pośrednio podważają zasadność zawartego w tej decyzji stwierdzenia Komisji o istnieniu odpowiedniego stopnia ochrony.

166. Moim zdaniem, w świetle okoliczności wynikających z powyższej analizy, wyjaśnienia Trybunału dotyczące tych zagadnień nie mogą zmienić jego wniosku odnoszącego się do ważności *in abstracto* decyzji 2010/87, ani w związku z tym mieć wpływu na rozstrzygnięcie sporu w postępowaniu głównym (część 1). Poza tym, o ile odpowiedzi Trybunału na te pytania mogłyby na późniejszym etapie okazać się użyteczne dla DPC dla potrzeb ustalenia (w ramach postępowania leżącego u podstaw tego sporu), czy rozpatrywane przekazywanie danych, *in concreto*, należy wstrzymać z uwagi na zarzut braku odpowiednich zabezpieczeń, to moim zdaniem rozstrzyganie tych zagadnień w ramach niniejszej sprawy byłoby przedwczesne (część 2).

1. W przedmiocie braku potrzeby udzielania odpowiedzi przez Trybunał z uwagi na przedmiot sporu w postępowaniu głównym

167. Należy przypomnieć, że spór w postępowaniu głównym wynika z faktu skorzystania przez DPC ze środka ochrony prawnej opisanego w pkt 65 wyroku Schrems, zgodnie z którym każde państwo członkowskie winno umożliwić organowi nadzorczemu, w sytuacji gdy uzna on za niezbędne do rozpatrzenia wniesionej doń skargi wystąpienie do sądu krajowego, aby ten zwrócił się do Trybunału z pytaniem prejudycjalnym w sprawie ważności decyzji stwierdzającej odpowiedni stopień ochrony czy też, analogicznie, decyzji ustanawiającej standardowe klauzule umowne.

168. High Court (wysoki trybunał) podkreślił w związku z tym, że po tym, gdy wystąpił do niego DPC, miał on do wyboru jedynie: bądź zwrócić się z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym co do ważności decyzji 2010/87, o co wnosił DPC (w przypadku, gdyby podzielał wątpliwości DPC dotyczące ważności tej decyzji), bądź, w przeciwnym razie, odmówić wystąpienia z takim wnioskiem. Sąd ten twierdzi, że, gdyby przyjął to drugie rozwiązanie, musiałby umorzyć postępowanie, ponieważ skarga DPC nie miała innego przedmiotu⁶⁷.

169. W podobny sposób, Supreme Court (sąd najwyższy), rozpoznając środek zaskarżenia wniesiony przez Facebook Ireland od postanowienia odsyłającego, opisał spór w postępowaniu głównym jako zapoczątkowany powództwem o ustalenie, w ramach którego DPC wnosi do sądu odsyłającego o przedłożenie Trybunałowi pytania prejudycjalnego co do ważności decyzji 2010/87. Zdaniem irlandzkiego sądu najwyższego, jedyne istotne zagadnienie podniesione przed sądem odsyłającym i przed nim samym dotyczy zatem ważności tej decyzji⁶⁸.

⁶⁶ Zobacz pkt 175 niniejszej opinii.

⁶⁷ Wyrok High Court (wysokiego trybunału) z dnia 3 października 2017 r. (pkt 337).

⁶⁸ Zgodnie z wyrokiem Supreme Court (sądu najwyższego) z dnia 31 maja 2019 r. (pkt 2.7), „[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFUE]”. Nawiązuje do tego pkt 2.9 tego wyroku: „Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter” (wyróżnienie moje).

170. Mając na względzie tak określony przedmiot sporu w postępowaniu głównym, sąd odsyłający przedłożył Trybunałowi dziesięć pierwszych pytań, ponieważ uznał, że ich analiza będzie przydatna do ogólnej oceny niezbędnej do tego, aby Trybunał mógł się wypowiedzieć (w odpowiedzi na pytanie jedenaste) co do ważności decyzji 2010/87 w świetle art. 7, 8 i 47 karty. Zgodnie z brzmieniem postanowienia odsyłającego pytanie to stanowi logiczną konsekwencję poprzedzających je pytań.

171. Z tego punktu widzenia, pytania od drugiego do piątego oraz pytania dziewiąte i dziesiąte są, jak się wydaje, oparte na założeniu, zgodnie z którym ważność decyzji 2010/87 miałaby zależeć od stopnia ochrony praw podstawowych, jaki został przewidziany w każdym z państw trzecich, do którego dane mogą zostać przekazane na podstawie zawartych w niej standardowych klauzul umownych. Tymczasem, jak wynika z mojej analizy pytania siódmego⁶⁹, założenie to jest według mnie błędne. Badanie prawa docelowego państwa trzeciego ma znaczenie wyłącznie w sytuacji, gdy Komisja przyjmuje decyzję stwierdzającą odpowiedni stopień ochrony lub gdy administrator – albo, w razie braku działania z jego strony, właściwy organ nadzorczy – weryfikuje, czy, w ramach przekazywania danych w oparciu o odpowiednie zabezpieczenia w rozumieniu art. 46 ust. 1 RODO, obowiązki, jakie prawo tego państwa trzeciego nakłada na podmiot odbierający dane, nie stanowią zagrożenia dla skuteczności ochrony zapewnianej przez te zabezpieczenia.

172. W konsekwencji, odpowiedzi Trybunału na powyższe pytania nie mogą wpłynąć na jego wnioski odnoszące się do pytania jedenastego⁷⁰. W związku z tym, mając na względzie przedmiot sporu w postępowaniu głównym oraz moją analizę pytania siódmego, nie ma potrzeby udzielania na nie odpowiedzi.

173. Proponuję Trybunałowi, aby ograniczył rozpoznawanie niniejszej sprawy adekwatnie do przedmiotu tego sporu. Moim zdaniem Trybunał powinien, rozpatrzyć pytania prejudycjalne w kontekście zawisłego przed DPC postępowania, które leży u ich podstaw, nie wykraczając poza to, co jest wymagane dla rozstrzygnięcia tego sporu. Jak wyjaśnię poniżej, to wezwanie do ograniczenia wynika, po pierwsze, z dbałości o to, by nie uprzedzać wyników normalnego postępowania, które będzie musiało być kontynuowane przed DPC po wydaniu przez Trybunał orzeczenia co do ważności decyzji 2010/87. Po drugie, w świetle okoliczności sprawy wydaje mi się, że badanie przez Trybunał problematyki poruszonej w pytaniach od drugiego do piątego oraz w pytaniach dziewiątym i dziesiątym byłoby nieco przedwcześnie, nawet z punktu widzenia celu, w jakim to postępowanie jest prowadzone.

2. Względy przemawiające przeciwko badaniu przez Trybunał pozostałych pytań w świetle przedmiotu toczącego się przed DPC postępowania

174. W skardze do DPC M. Schrems wnosi do tego organu nadzorczego, by skorzystał z uprawnień, którymi dysponuje na mocy art. 58 ust. 2 lit. f) RODO, nakazując spółce Facebook Ireland zawieszenie przekazywania dotyczących go danych osobowych do Stanów Zjednoczonych, dokonywanego w oparciu o standardowe klauzule umowne. Na poparcie tego wniosku M. Schrems podnosi zasadniczo, że te umowne zabezpieczenia są nieodpowiednie w kontekście będącej wynikiem działalności amerykańskich służb wywiadowczych ingerencji w korzystanie przez niego z jego praw podstawowych.

⁶⁹ Zobacz pkt 124 niniejszej opinii.

⁷⁰ Z tego samego powodu Supreme Court (sąd najwyższy) w wyroku z dnia 31 maja 2019 r. (pkt 8.1–8.5), uznając się za niewłaściwy do podważania wydanego przez sąd odsyłający orzeczenia o przedłożeniu Trybunałowi pytań prejudycjalnych oraz do wprowadzania zmian w ich brzmieniu, wyraził wątpliwości co do potrzeby zadawania niektórych spośród tych pytań. W szczególności, zgodnie z pkt 8.5 tego wyroku: „The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures [...]”.

175. Argumentacja M. Schremsa podważa stwierdzenie sformułowane przez Komisję w decyzji w sprawie Tarczy Prywatności, zgodnie z którym Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych przekazywanych na podstawie tej decyzji, biorąc pod uwagę ograniczenia, jakim został poddany dostęp do tych danych i ich wykorzystanie przez amerykańskie organy wywiadu, jak również ochronę prawną przysługującą osobom, których dane dotyczą⁷¹. Obawy wyrażone wstępnie przez DPC⁷² oraz przez sąd odsyłający w ramach czwartego, piątego i dziesiątego pytania pośrednio również rzucają cień wątpliwości na zasadność tego stwierdzenia.

176. Decyzja w sprawie Tarczy Prywatności niewątpliwie ogranicza się do stwierdzenia adekwatności stopnia ochrony danych osobowych przekazywanych zgodnie z wyrażonymi w niej zasadami przedsiębiorstwom mającym siedziby w Stanach Zjednoczonych, które dokonując samocertyfikacji zobowiązały się do przestrzegania tych zasad⁷³. Jednakże zawarte w niej rozważania wykraczają poza ramy przekazywania danych uregulowanego w tej decyzji, ponieważ odnoszą się one do prawa i praktyki obowiązujących w tym państwie trzecim w zakresie przetwarzania przekazanych danych osobowych na potrzeby ochrony bezpieczeństwa narodowego. Jak zauważyli zasadniczo Facebook Ireland, M. Schrems, rząd Stanów Zjednoczonych i Komisja, nadzór prowadzony przez amerykańskie organy wywiadu, podobnie jak zabezpieczenia przeciwko ryzykom nadużyć, jakie jego sprawowanie niesie ze sobą, oraz mechanizmy służące kontroli stosowania tych zabezpieczeń, mają zastosowanie niezależnie od tego, jaka jest (z punktu widzenia prawa Unii) wskazywana podstawa prawna tego przekazywania danych.

177. Z tej perspektywy pytanie dotyczące tego, czy ustalenia sformułowane na ten temat w decyzji w sprawie Tarczy Prywatności są wiążące dla organów nadzorczych, gdy badają one zgodność z prawem przekazywania danych odbywającego się w oparciu o standardowe klauzule umowne, mogłoby okazać się istotne na potrzeby rozpatrzenia przez DPC skargi M. Schremsa. Gdyby została na nie udzielona odpowiedź twierdząca, powstałoby pytanie, czy decyzja ta w istocie jest ważna.

178. Nie zalecam jednakże Trybunałowi, aby orzekał w przedmiocie tych pytań wyłącznie w celu udzielenia DPC pomocy w rozpatrywaniu tej skargi w sytuacji, gdy nie ma potrzeby odpowiadania na nie w celu umożliwienia sądowi odsyłającemu rozstrzygnięcia sporu w postępowaniu głównym. Skoro przewidziane w art. 267 TFUE postępowanie opiera się na dialogu między sądami, rolą Trybunału nie jest dostarczanie wyjaśnień wyłącznie w celu udzielenia wsparcia organowi administracji w ramach postępowania leżącego u podstaw tego sporu.

179. Moim zdaniem ostrożność jest wskazana tym bardziej, że Trybunałowi nie zostało w sposób jednoznaczny zadane pytanie dotyczące ważności decyzji w sprawie Tarczy Prywatności – a poza tym, decyzja ta jest już przedmiotem rozpatrywanej przez Sąd Unii Europejskiej skargi o stwierdzenie nieważności⁷⁴.

71 Zobacz motywy 64–141 decyzji w sprawie Tarczy Prywatności. Przypomnę, że, jak wynika z art. 1 ust. 2 tej decyzji, na Tarczę Prywatności składają się nie tylko zasady, których zobowiązały się przestrzegać przedsiębiorstwa zamierzające przekazywać dane na podstawie rzeczonyj decyzji, lecz również uzyskane od rządu Stanów Zjednoczonych oficjalne oświadczenia i zobowiązania zawarte w dokumentach załączonych do tej decyzji.

72 Projekt decyzji DPC jest wcześniejszy niż decyzja w sprawie Tarczy Prywatności. DPC wyjaśnił w tym projekcie, że, chociaż wstępnie przyjął, iż zabezpieczenia przewidziane w prawie Stanów Zjednoczonych co najmniej nie umożliwiają zapewnienia zgodności przekazywania danych do tego państwa co najmniej z art. 47 karty, *to nie badał on ani nie uwzględnił na tym etapie nowych uzgodnień rozważanych w projekcie porozumienia dotyczącego Tarczy Prywatności, ponieważ nie zostało ono jeszcze zawarte*. Jednakże w pkt 307 wyroku z dnia 3 października 2017 r., High Court (wysoki trybunał) stwierdził: „It is fair to conclude [...] that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U.S.], conflicts with the case made by the DPC to this court”.

73 Zobacz art. 1 ust. 1 i 3 oraz motywy 14–16 decyzji w sprawie Tarczy Prywatności.

74 Będąca w toku sprawa T-738/16, La Quadrature du Net i in./Komisja (Dz.U. 2017, C 6, s. 39).

180. Ponadto, wypowiadając się w przedmiocie tej problematyki, Trybunał spowodowałby moim zdaniem zakłócenie zwykłego biegu postępowania, jakie powinno zostać przeprowadzone po wydaniu przezeń wyroku w niniejszej sprawie. W ramach tego postępowania DPC będzie miał za zadanie rozpatrzyć skargę M. Schremsa z uwzględnieniem odpowiedzi udzielonej przez Trybunał na jedenaste pytanie prejudycjalne. Jeżeli Trybunał orzeknie, tak jak proponuję i wbrew twierdzeniom, jakie przedstawił DPC przed Trybunałem, a mianowicie, że decyzja 2010/87 nie jest nieważna w świetle art. 7, 8 i 47 karty, w mojej ocenie DPC powinien uzyskać możliwość ponownego przeanalizowania aktu toczącego się przed nim postępowania. W przypadku gdy DPC uznałby, że nie jest w stanie wydać rozstrzygnięcia w przedmiocie skargi M. Schremsa bez uprzedniego ustalenia przez Trybunał, czy decyzja w sprawie Tarczy Prywatności stoi na przeszkodzie skorzystaniu przez ten organ z przysługującego mu uprawnienia do zawieszenia przekazywania danych, którego dotyczy sprawa, i potwierdziłby żywione wątpliwości co do ważności tej decyzji, miałby on możliwość ponownego wystąpienia do sądu krajowego, aby ten zwrócił się do Trybunału z pytaniem w tej sprawie⁷⁵.

181. Zostałoby wtedy wszczęte postępowanie umożliwiające wszystkim stronom i zainteresowanym podmiotom, o których mowa w art. 23 akapit drugi statutu Trybunału, przedłożenie mu uwag dotyczących konkretnie kwestii ważności decyzji w sprawie Tarczy Prywatności oraz wskazanie w razie potrzeby poszczególnych ustaleń, które kwestionują oraz powodów, dla których uważają, że Komisja przekroczyła w niej ograniczony zakres uznania, jakim dysponowała⁷⁶. W ramach takiego postępowania Komisja miałaby możliwość udzielenia wyczerpujących i szczegółowych odpowiedzi na każde z ewentualnych zastrzeżeń skierowanych przeciwko tej decyzji. Chociaż niniejsza sprawa umożliwiła stronom i zainteresowanym podmiotom, które przedłożyły Trybunałowi uwagi, przedyskutowanie niektórych aspektów istotnych dla oceny zgodności decyzji w sprawie Tarczy Prywatności z art. 7, 8 i 47 karty, to jednak zagadnienie to, ze względu na jego wagę, zasługuje na to, aby została mu poświęcona wyczerpująca i pogłębiona dyskusja.

182. Moim zdaniem ostrożność wymaga, aby Trybunał zaczekał, aż zakończą się te etapy postępowania, aby dopiero potem zbadać wpływ, jaki wywiera decyzja w sprawie Tarczy Prywatności na rozpatrzenie przez organ nadzorczy wniosku o zawieszenie przekazywania danych do Stanów Zjednoczonych na podstawie art. 46 ust. 1 RODO i wypowiedzieć się co do ważności tej decyzji.

183. Jest to zasadne tym bardziej, że z aktu sprawy przedłożonych Trybunałowi nie można wywnioskować, iż sposób rozpatrzenia skargi M. Schremsa przez DPC będzie z pewnością zależał od ustalenia tego, czy decyzja w sprawie Tarczy Prywatności stoi na przeszkodzie skorzystaniu przez organy nadzorcze z uprawnień do zawieszenia przekazywania danych w oparciu o standardowe klauzule umowne.

184. W tym względzie, po pierwsze, nie można wykluczyć, że DPC zdecyduje się zawiesić przekazywanie danych, którego dotyczy sprawa, z innych przyczyn niż te związane z zarzutem, że w Stanach Zjednoczonych nie zapewnia się odpowiedniego stopnia ich ochrony przed naruszeniami praw podstawowych osób, których dane dotyczą, wynikającymi z działań amerykańskich służb wywiadowczych. W szczególności sąd odsyłający wyjaśnił, że M. Schrems twierdzi w swojej skardze do DPC, iż klauzule umowne wskazane przez Facebook Ireland jako podstawa przekazywania danych nie odzwierciedlają dokładnie klauzul zawartych w załączniku do decyzji 2010/87. Maximilian Schrems twierdzi ponadto, że rozpatrywane przekazywanie danych nie jest objęte zakresem stosowania tej decyzji, lecz innych decyzji w sprawie standardowych klauzul umownych⁷⁷.

⁷⁵ Chciałbym ponadto zauważyć, że w swoich uwagach na piśmie DPC nie zajął stanowiska co do wpływu decyzji w sprawie Tarczy Prywatności na rozpatrzenie wniesionej do niego skargi.

⁷⁶ Zobacz w tym względzie wyrok Schrems (pkt 78).

⁷⁷ Na poparcie tego twierdzenia M. Schrems podnosi, że spółkę Facebook Inc., należy w związku z przetwarzaniem danych osobowych użytkowników sieci społecznościowej Facebook uznać nie tylko za podmiot przetwarzający, lecz również za administratora w rozumieniu art. 4 pkt 7 RODO. Zobacz w tym względzie wyrok z dnia 5 czerwca 2018 r., Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, pkt 30).

185. Po drugie, DPC i sąd odsyłający podkreślili, że Facebook Ireland nie wskazała decyzji w sprawie Tarczy Prywatności jako podstawy przekazywania danych, których dotyczy skarga M. Schremsa⁷⁸, co zostało potwierdzone przez tę spółkę w trakcie rozprawy. Mimo że Facebook Inc. poprzez samocertyfikację zobowiązała się przestrzegać zasad Tarczy Prywatności od dnia 30 września 2016 r.⁷⁹, Facebook Ireland twierdzi, że to zobowiązanie odnosi się wyłącznie do pewnych kategorii danych, a mianowicie tych, które dotyczą partnerów handlowych Facebook Inc. Nie wydaje mi się właściwe, aby Trybunał uprzedzał wątpliwości, jakie mogłyby powstać w tym względzie przy okazji analizowania tego, czy w przypadku, gdyby Facebook Ireland nie mogłaby wskazać decyzji 2010/87 jako podstawy rozpatrywanego przekazywania danych, przekazywanie to byłoby jednak objęte decyzją w sprawie Tarczy Prywatności, skoro nawet ta spółka nie podniosła tego argumentu ani przed sądem odsyłającym ani przed DPC.

186. Wnioskuje z tego, że nie ma potrzeby udzielania odpowiedzi na pytania od drugiego do piątego oraz na pytania dziewiąte i dziesiąte, ani też badania ważności decyzji w sprawie Tarczy Prywatności.

G. Uwagi uzupełniające dotyczące skutków i ważności decyzji w sprawie Tarczy Prywatności

187. Mimo że powyższa analiza skłania mnie przede wszystkim do zaproponowania Trybunałowi, aby wstrzymał się od orzekania co do wpływu decyzji w sprawie Tarczy Prywatności na rozpatrzenie skargi wniesionej do DPC przez M. Schremsa oraz co do ważności tej decyzji, uznałem za użyteczne przedstawienie, tytułem uzupełnienia, kilku niewyczerpujących i zawierających zastrzeżenia uwag na ten temat.

1. Wpływ decyzji w sprawie Tarczy Prywatności na rozpatrywanie przez organ nadzorczy skargi dotyczącej zgodności z prawem przekazywania danych w oparciu o zabezpieczenia umowne

188. Dziewiąte pytanie prejudycjalne dotyczy kwestii, czy zawarte w decyzji w sprawie Tarczy Prywatności ustalenia dotyczące adekwatności stopnia ochrony, jaki zapewniają Stany Zjednoczone (w świetle ograniczeń dotyczących dostępu do przekazywanych danych i ich wykorzystywania przez organy amerykańskie do celów bezpieczeństwa narodowego) i ochrony prawnej osób, których dane dotyczą, sprzeciwiają się zawieszeniu przez organ nadzorczy przekazywania danych do tego państwa w oparciu o standardowe klauzule umowne.

189. Uważam, iż zagadnienie to należy rozpatrywać w świetle pkt 51 i 52 wyroku Schrems, z których wynika, że decyzja stwierdzająca odpowiedni stopień ochrony jest wiążąca dla organów nadzorczych tak długo, dopóki nie zostanie stwierdzona jej nieważność. Organ nadzorczy rozpatrujący skargę osoby, której dane są przekazywane do państwa trzeciego wskazanego w decyzji stwierdzającej odpowiedni stopień ochrony, nie może zatem zawiesić przekazywania danych na tej podstawie, że stopień ochrony w tym państwie nie jest odpowiedni, bez wcześniejszego stwierdzenia nieważności tej decyzji przez Trybunał⁸⁰.

190. Sąd odsyłający chciałby w istocie ustalić, czy w odniesieniu do decyzji stwierdzającej odpowiedni stopień ochrony – takiej jak decyzja w sprawie Tarczy Prywatności, czy też, wcześniej, decyzja w sprawie bezpiecznej przystani – opierającej się na dobrowolnym zobowiązaniu się przedsiębiorstw do przestrzegania wyrażonych w niej zasad, wniosek ten ma zastosowanie wyłącznie w sytuacji, gdy przekazywanie danych do tego państwa trzeciego jest objęte tą decyzją, czy także w sytuacji, gdy jest dokonywane na odrębnej podstawie prawnej.

⁷⁸ Zobacz wyrok High Court (wysokiego trybunału) z dnia 3 października 2017 r. (pkt 66).

⁷⁹ Zobacz stronę internetową Tarczy Prywatności (https://www.privacyshield.gov/participant_search).

⁸⁰ Zobacz podobnie wyrok Schrems (pkt 59).

191. Zdaniem M. Schremsa, rządów niemieckiego, niderlandzkiego, polskiego i portugalskiego oraz Komisji, zawarte w decyzji w sprawie Tarczy Prywatności stwierdzenie dotyczące odpowiedniego stopnia ochrony nie pozbawia organów nadzorczych ich uprawnienia do zawieszenia lub zakazania przekazywania danych do Stanów Zjednoczonych, które odbywa się na podstawie standardowych klauzul umownych. W sytuacji, gdy to przekazywanie danych do Stanów Zjednoczonych nie jest dokonywane w oparciu o decyzję w sprawie Tarczy Prywatności, organy nadzorcze w ramach wykonywania uprawnień powierzonych im na podstawie art. 58 ust. 2 RODO nie są formalnie związane tą decyzją. Innymi słowy, organy te mogłyby zdystansować się od poczynionych przez Komisję ustaleń w przedmiocie odpowiedniego stopnia ochrony przed ingerencjami ze strony amerykańskich organów władz publicznych w korzystanie z praw podstawowych przez osoby, których dane dotyczą. Rząd niderlandzki i Komisja wyjaśniają, że organy nadzorcze, korzystając z tych uprawnień, powinny jednak brać pod uwagę powyższe ustalenia. Zdaniem rządu niemieckiego organy te mogłyby dokonać odmiennej oceny wyłącznie po przeprowadzeniu merytorycznego badania ustaleń poczynionych przez Komisję, obejmującego odpowiednie dochodzenie.

192. Natomiast Facebook Ireland i rząd Stanów Zjednoczonych twierdzą zasadniczo, że moc wiążąca decyzji stwierdzającej odpowiedni stopień ochrony, w związku z wymogami pewności prawa i jednolitego stosowania prawa Unii, skutkuje tym, że organy nadzorcze, nawet w ramach rozpatrywania skargi mającej na celu spowodowanie zawieszenia przekazywania danych do danego państwa trzeciego, odbywającego się na innej podstawie niż ta decyzja, nie są uprawnione do kwestionowania stwierdzeń zawartych w rzeczowej decyzji.

193. Przychyłam się do pierwszego z tych dwóch stanowisk. Ponieważ zakres stosowania decyzji w sprawie Tarczy Prywatności jest ograniczony do przekazywania danych dokonywanego do samocertyfikowanego na podstawie tej decyzji przedsiębiorstwa, decyzja ta nie może formalnie wiązać organów nadzorczych, jeśli chodzi o przekazywanie danych, które nie jest objęte zakresem jej stosowania. Decyzja w sprawie Tarczy Prywatności ma odpowiednio na celu zapewnienie pewności prawa wyłącznie podmiotom przekazującym dane, które przekazują je w ustanowionych przez nią ramach. W mojej ocenie, niezależność, jaką art. 52 RODO przyznaje organom nadzorczym, ma również na celu przeszkodzenie temu, by organy te były związane ustaleniami poczynionymi przez Komisję w decyzji stwierdzającej odpowiedni stopień ochrony w kwestiach nieobjętych zakresem jej stosowania.

194. Jest oczywiste, że ustalenia zawarte w decyzji w sprawie Tarczy Prywatności odnoszące się do tego, czy w Stanach Zjednoczonych zapewnia się odpowiedni stopień ochrony przed ingerencjami związanymi z działaniami ich służb wywiadowczych, stanowią punkt wyjścia dla analizy, w ramach której organ nadzorczy ocenia, indywidualnie dla każdego przypadku, czy przekazywanie danych w oparciu o standardowe klauzule umowne powinno zostać zawieszone z powodu takich ingerencji. Jednakże jeżeli właściwy organ nadzorczy po przeprowadzeniu pogłębionej analizy uzna, że nie może się zgodzić z tymi ustaleniami, jeśli chodzi o poddane jego ocenie przekazywanie danych, organ ten zachowuje według mnie możliwość skorzystania z uprawnień, jakie daje mu art. 58 ust. 2 lit. f) i j) RODO.

195. Jednakże, na wypadek, gdyby Trybunał zamierzał udzielić na analizowane w tym miejscu pytanie odpowiedzi odmiennej od tej, którą proponuję, należałoby zbadać, czy uprawnienia te nie powinny zostać przywrócone z uwagi na nieważność decyzji w sprawie Tarczy Prywatności.

2. W przedmiocie ważności decyzji w sprawie Tarczy Prywatności

196. W ramach dalszych uwag zostaną podniesione pewne wątpliwości co do zasadności ocen zawartych decyzji w sprawie Tarczy Prywatności, dotyczących odpowiedniego charakteru stopnia ochrony (w rozumieniu art. 45 ust. 1 RODO), jaki zapewniają Stany Zjednoczone w związku z prowadzeniem przez amerykańskie organy wywiadu nadzoru komunikatów elektronicznych. Celem

tych uwag nie jest przedstawienie ostatecznego ani wyczerpującego stanowiska co do ważności tej decyzji. Ograniczę się w nich do przekazania pewnych refleksji, które mogłyby okazać się użyteczne dla Trybunału w przypadku, gdyby (wbrew temu, co proponuję) zdecydował się orzekać w tym przedmiocie.

197. Z motywu 64 oraz pkt I.5 załącznika II do decyzji w sprawie Tarczy Prywatności wynika w tym względzie, że przestrzeganie przez przedsiębiorstwa zasad wyrażonych w tej decyzji może być ograniczone w szczególności ze względu na wymogi bezpieczeństwa narodowego, interesu publicznego lub egzekwowania prawa lub ze względu na sprzeczność z obowiązkami wynikającymi z prawa amerykańskiego.

198. W związku z tym Komisja oceniła przewidziane w prawie Stanów Zjednoczonych zabezpieczenia w zakresie dotyczącym dostępu do przekazywanych danych i ich wykorzystania przez amerykańskie organy publiczne, w szczególności na potrzeby bezpieczeństwa narodowego⁸¹. Komisja uzyskała od rządu amerykańskiego pewnie zobowiązania dotyczące, po pierwsze, ograniczeń odnośnie do dostępu do przekazywanych danych, jaki uzyskują organy amerykańskich władz, a także sposobu ich wykorzystywania, i, po drugie, ochrony prawnej przyznanej osobom, których te dane dotyczą⁸².

199. Maximilian Schrems podniósł przed Trybunałem, że decyzja w sprawie Tarczy Prywatności jest nieważna, ponieważ opisane w ten sposób zabezpieczenia nie są wystarczające dla zapewnienia odpowiedniego stopnia ochrony praw podstawowych osób, których dane są przekazywane do Stanów Zjednoczonych. DPC, EPIC oraz rządy austriacki, polski i portugalski, nie podważając bezpośrednio ważności tej decyzji, kwestionują dokonane w niej przez Komisję oceny dotyczące odpowiedniego stopnia ochrony przed ingerencjami wynikającymi z działań amerykańskich służb wywiadowczych. Wątpliwości te znajdują odzwierciedlenie w obawach wyrażanych przez Parlament⁸³, EROD⁸⁴ i Europejskiego Inspektora Ochrony Danych⁸⁵.

200. Przed przystąpieniem do badania zasadności ustalenia dotyczącego odpowiedniego stopnia ochrony zawartego w decyzji w sprawie Tarczy Prywatności, należy przybliżyć metodologię, jaka powinna być zastosowana do tego badania.

81 Zobacz motyw 65 decyzji w sprawie Tarczy Prywatności.

82 Zobacz załączniki III–VII do decyzji w sprawie Tarczy Prywatności.

83 Rezolucje Parlamentu Europejskiego z dnia 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez tzw. Tarczę Prywatności UE–USA, P8_TA(2017)0131 i z dnia 5 lipca 2018 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, P8_TA-PROV(2018)0315.

84 Zobacz opinie grupy roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych utworzonej na podstawie art. 29 (zwanej dalej „grupą roboczą z art. 29”), Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 13 kwietnia 2016 r., WP 238; grupa robocza z art. 29, EU-US Privacy Shield – First Annual Joint Review, 28 listopada 2017 r., WP 255; EROD, EU-US Privacy Shield – Second Annual Joint Review, 22 stycznia 2019 r. Grupa robocza z art. 29 została powołana na mocy art. 29 ust. 1 dyrektywy 95/46, który stanowił, że będzie ona miała charakter doradczy i będzie działała w sposób niezależny. Zgodnie z ust. 2 tego artykułu, w skład grupy roboczej wchodził przedstawiciel organu nadzorczego każdego z państw członkowskich, przedstawiciel organu ustanowionego dla instytucji i organów wspólnotowych, oraz przedstawiciel Komisji. Od chwili wejścia w życie RODO grupa robocza z art. 29 została zastąpiona przez EROD (zob. art. 94 ust. 2 tego rozporządzenia).

85 Zobacz opinie 4/2016 Europejskiego Inspektora Ochrony danych dotyczącą Tarczy Prywatności UE–Stany Zjednoczone (Privacy Shield) – Projekt decyzji z dnia 30 maja 2016 r. stwierdzającej odpowiedni stopień ochrony. Urząd Europejskiego Inspektora Ochrony Danych został ustanowiony na mocy art. 1 ust. 2 rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. 2001, L 8, s. 1 – wyd. spec. w jęz. polskim, rozdz. 13, t. 26, s. 102). Monitoruje on stosowanie przepisów tego rozporządzenia.

a) Wyjaśnienia dotyczące zakresu badania ważności decyzji stwierdzającej odpowiedni stopień ochrony

1) W przedmiocie kryteriów porównawczych umożliwiających ocenę merytorycznej równoważności stopnia ochrony

201. Zgodnie z art. 45 ust. 3 RODO oraz z orzecznictwem Trybunału⁸⁶, Komisja może uznać, że państwo trzecie zapewnia odpowiedni stopień ochrony wyłącznie wówczas, jeżeli w należycie uzasadniony sposób stwierdzi, iż stopień ochrony praw podstawowych osób, których dane dotyczą, jest w tym państwie „pod względem merytorycznym” równoważny ze stopniem ochrony wymaganym w Unii zgodnie z tym rozporządzeniem w związku z kartą.

202. W związku z tym do weryfikacji tego, czy w danym państwie zapewniony jest odpowiedni stopień ochrony, konieczne jest przeprowadzenie porównania zasad, które obowiązują w tym państwie trzecim, oraz stosowanych w nim praktyk, ze standardami ochrony obowiązującymi w Unii. W drugim pytaniu prejudycjalnym sąd odsyłający zwraca się do Trybunału o wskazanie kryteriów mających służyć przeprowadzeniu takiego porównania⁸⁷.

203. Ścisłej rzecz ujmując, sąd ten stara się ustalić, czy zastrzeżenie na rzecz państw członkowskich kompetencji w dziedzinie ochrony bezpieczeństwa narodowego wynikające z art. 4 ust. 2 TUE i art. 2 ust. 2 RODO skutkuje tym, że porządek prawny Unii nie przewiduje standardów ochrony, które stanowiłyby punkt odniesienia dla porównania, w ramach oceny ich adekwatności, zapewnianych w państwie trzecim zabezpieczeń odnoszących się do przetwarzania przez organy władz publicznych (w celach związanych z ochroną bezpieczeństwa narodowego) danych, które są im przekazywane. W przypadku udzielenia odpowiedzi twierdzącej, sąd ten chciałby się dowiedzieć, w jaki sposób należy określić te właściwe ramy odniesienia.

204. Należy w tym względzie pamiętać, że powodem, dla którego prawo Unii nakłada ograniczenia na międzynarodowe transfery danych osobowych, wymagając zapewnienia ciągłości stopnia ochrony praw osób, których te dane dotyczą, jest ograniczanie ryzyka obchodzenia standardów mających zastosowanie w Unii⁸⁸. Jak zasadniczo podniosła Facebook Ireland, w świetle tego celu oczekiwanie, że państwo trzecie będzie przestrzegało wymogów, które nie harmonizują z obowiązkami ciążącymi na państwach członkowskich, byłoby zupełnie nieuzasadnione.

205. Zgodnie zaś z art. 51 ust. 1 karty akt ten ma ona zastosowanie do państw członkowskich wyłącznie w zakresie, w jakim wdrażają one prawo Unii. W konsekwencji ważność decyzji stwierdzającej odpowiedni stopień ochrony w związku z ograniczeniami wynikającymi z przepisów docelowego państwa trzeciego, w zakresie dotyczącym korzystania z praw podstawowych przez osoby, których dane dotyczą, zależy od porównania tych ograniczeń z ograniczeniami, na które pozwalałyby państwom członkowskim postanowienia karty, *wyłącznie w sytuacji, gdyby podobne przepisy w państwie członkowskim były objęte zakresem stosowania prawa Unii.*

⁸⁶ Zobacz pkt 112 niniejszej opinii.

⁸⁷ Przypominam, że porównanie merytorycznej równoważności stopnia ochrony, jaki zapewnia państwo trzecie, ze stopniem ochrony, jaki jest wymagany w Unii, należy również przeprowadzić w sytuacji, gdy w ramach konkretnego przekazywania danych w oparciu o standardowe klauzule umowne przewidziane w decyzji 2010/87, administrator lub, w razie jego beczynności, właściwy organ nadzorczy sprawdza, czy organy władz publicznych docelowego państwa trzeciego nakładają na podmiot odbierający dane wymogi wykraczające poza to, co jest niezbędne w demokratycznym społeczeństwie (zob. klauzulę 5 w załączniku do decyzji 2010/87 oraz odnoszący się do niej przypis). Zobacz pkt 115, 134 i 135 niniejszej opinii.

⁸⁸ Zobacz pkt 117 niniejszej opinii.

206. Jednakże nie można oceniać adekwatności stopnia ochrony, jaki zapewnia docelowe państwo trzecie, z pominięciem ewentualnych ingerencji w korzystanie przez osoby, których dane są przekazywane, z praw podstawowych, które to ingerencje wynikają z państwowych aktów prawnych, w szczególności przyjmowanych w dziedzinie bezpieczeństwa narodowego, które to akty, gdyby były przyjęte przez państwo członkowskie, leżałyby poza zakresem stosowania prawa Unii. Artykuł 45 ust. 2 lit. a) RODO wymaga, aby na potrzeby tej oceny brać pod uwagę, bez jakichkolwiek ograniczeń, ustawodawstwo w dziedzinie bezpieczeństwa narodowego obowiązujące w tym państwie trzecim.

207. Moim zdaniem, ocena odpowiedniego charakteru stopnia ochrony w związku z takimi państwowymi aktami prawnymi wymaga przeprowadzenia porównania zabezpieczeń, które im towarzyszą, ze stopniem ochrony wymagany w Unii na podstawie prawa państw członkowskich, w tym ich zobowiązań wynikających z EKPC. Skoro przystąpienie państw członkowskich do EKPC zobowiązuje je do dostosowania ich prawa wewnętrznego do postanowień tej konwencji i stanowi (jak zasadniczo podkreślili Facebook Ireland, rządy niemiecki i czeski oraz Komisja), wspólny mianownik dla państw członkowskich, będę uznawał jej postanowienia za odpowiednie, dla potrzeb przeprowadzenia tej oceny, kryterium porównawcze.

208. Jak wcześniej zauważyłem⁸⁹, w tym wypadku wymogi związane z bezpieczeństwem narodowym Stanów Zjednoczonych mają pierwszeństwo przed zobowiązaniami podjętymi przez przedsiębiorstwa w drodze samocertyfikacji na podstawie decyzji w sprawie Tarczy Prywatności. W związku z tym ważność tej decyzji zależy od tego, czy wymogom tym towarzyszą zabezpieczenia zapewniające stopień ochrony równoważny pod względem merytorycznym z tym, jaki powinien być zapewniany w Unii.

209. Udzielenie odpowiedzi na to pytanie wymaga w pierwszej kolejności wskazania standardów – wywiedzionych z karty lub EKPC – którym powinny odpowiadać w Unii przepisy dotyczące nadzorowania komunikatów elektronicznych podobne do przepisów, które były analizowane przez Komisję w decyzji w sprawie Tarczy Prywatności. Określenie mających zastosowanie standardów zależy od ustalenia, czy przepisy takie jak art. 702 FISA i EO 12333 – gdyby pochodziły od państwa członkowskiego – byłyby wyłączone z zakresu stosowania RODO na podstawie art. 2 ust. 2 tego rozporządzenia w związku z art. 4 ust. 2 TUE.

210. Z art. 4 ust. 2 TUE oraz z utrwalonego orzecznictwa wynika w tym względzie, że prawo Unii, a w szczególności akty prawa wtórnego dotyczące ochrony danych osobowych, nie mają zastosowania do działań w obszarze ochrony bezpieczeństwa narodowego, ponieważ są to działania właściwe państwom i władzom państwowym, odmienne od dziedzin działalności jednostek⁹⁰.

211. Zasada ta oznacza, z *jednej strony*, że ustawodawstwo w obszarze ochrony bezpieczeństwa narodowego nie jest objęte zakresem stosowania prawa Unii, gdy reguluje ono wyłącznie działania państwa i nie obejmuje jakichkolwiek działań podejmowanych przez jednostki. W konsekwencji, prawo Unii nie ma według mnie zastosowania do uregulowań krajowych wprowadzanych bezpośrednio przez państwo w celu ochrony bezpieczeństwa narodowego, które odnoszą się do gromadzenia i wykorzystywania danych osobowych, nie nakładając konkretnych obowiązków na podmioty

⁸⁹ Zobacz pkt 197 niniejszej opinii.

⁹⁰ Zobacz w szczególności wyrok z dnia 6 listopada 2003 r., Lindqvist (C-101/01, EU:C:2003:596, pkt 43 i 44); wyrok PNR (pkt 58); wyrok z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia (C-73/07, EU:C:2008:727, pkt 41); wyrok z dnia 21 grudnia 2016 r., Tele2 Sverige i Watson i in. (sprawy połączone C-203/15 i C-698/15, EU:C:2016:970, zwany dalej „wyrokiem Tele2 Sverige”, pkt 69); wyrok z dnia 2 października 2018 r., Ministerio Fiscal (C-207/16, EU:C:2018:788, zwany dalej „wyrokiem Ministerio Fiscal”, pkt 32).

prywatne. W szczególności, jak podniosła Komisja podczas rozprawy, przyjęty przez państwo członkowskie przepis, który, tak jak EO 12333, upoważniałby jego służby bezpieczeństwa do uzyskiwania bezpośredniego dostępu do danych „w tranzycie”, byłby wyłączony z zakresu stosowania prawa Unii⁹¹.

212. Znacznie bardziej złożona jest kwestia ustalenia, czy, z *drugiej strony*, przepisy krajowe, które, tak jak art. 702 FISA, zobowiązują dostawców usług łączności elektronicznej do udzielania wsparcia organom właściwym w dziedzinie bezpieczeństwa narodowego poprzez umożliwienie im uzyskania dostępu do niektórych danych osobowych, również byłyby wyłączone z zakresu stosowania prawa Unii.

213. O ile wyrok PNR przemawia za udzieleniem odpowiedzi twierdzącej na to pytanie, rozumowanie zastosowane w wyrokach Tele2 Sverige i Ministerio Fiscal mogłoby uzasadniać udzielenie na nie odpowiedzi przeczącej.

214. W wyroku PNR Trybunał stwierdził nieważność decyzji, w której Komisja uznała, że stopień ochrony danych osobowych dotyczących pasażerów lotniczych zawartych w Passenger Name Records (PNR) przekazywanych amerykańskiemu organowi właściwemu w sprawach cel i ochrony granic, jest odpowiedni⁹². Trybunał orzekł, że przetwarzanie danych, których dotyczyła ta decyzja – a mianowicie przekazywanie danych PNR temu organowi przez przewoźników lotniczych – jest, *ze względu na jego przedmiot*, objęte wyłączeniem z zakresu stosowania dyrektywy 95/46 przewidzianym w jej art. 3 ust. 2. Zdaniem Trybunału przetwarzanie tych danych było niezbędne nie w celu świadczenia usług, lecz w celu ochrony bezpieczeństwa publicznego i zwalczania przestępczości. Ponieważ rozpatrywane przekazywanie danych odbywało się w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego, było ono wyłączone z zakresu stosowania tej dyrektywy, mimo że dane PNR były pierwotnie zbierane przez podmioty prywatne w ramach ich działalności komercyjnej objętej zakresem jej stosowania oraz mimo że ich przekazywanie było organizowane przez te podmioty⁹³.

215. W późniejszym wyroku Tele2 Sverige⁹⁴ Trybunał orzekł, że przepisy krajowe oparte na art. 15 ust. 1 dyrektywy 2002/58/WE⁹⁵, regulujące zarówno zatrzymywanie danych o ruchu i lokalizacji przez dostawców usług telekomunikacyjnych jak też dostęp organów publicznych do zatrzymywanych danych w celach określonych w tym przepisie – wśród których znajduje się ściganie karne i ochrona

91 W celu uniknięcia wszelkich nieporozumień w tej kwestii, podkreślam, że Komisja w decyzji w sprawie Tarczy Prywatności nie była w stanie określić, czy Stany Zjednoczone rzeczywiście przechwytyują komunikaty, gdy podlegają one transferowi za pośrednictwem kabli transatlantycznych, ponieważ organy amerykańskie w żaden sposób nie ustosunkowały się do tego twierdzenia [zob. motyw 75 tej decyzji, jak również pkt I lit. a) pisma Roberta Litta z dnia 22 lutego 2016 r. znajdującego się w jej załączniku VI]. Skoro jednak rząd Stanów Zjednoczonych nie zaprzeczył temu, że, w oparciu o EO 12333, gromadzi dane w trakcie ich transferu, Komisja powinna była poprzedzić swe stwierdzenie, zgodnie z którym istniejący stopień ochrony ma odpowiedni charakter, powinna była, jak się wydaje, uzyskać od tego rządu zapewnienia, że takiemu gromadzeniu danych (gdyby do niego doszło), towarzyszyłyby dostateczne zabezpieczenia przed ryzykiem nadużyć. Właśnie z tej perspektywy Komisja zbadała w motywach 68–77 rzeczonyj decyzji ograniczenia i zabezpieczenia, które w takiej sytuacji powinny mieć zastosowanie na mocy PPD 28.

92 Chodziło o decyzję Komisji 2004/535/WE z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych (Dz.U. 2004, L 235, s. 11).

93 Wyrok PNR (pkt 56–58). Poza tym, w wyroku z dnia 10 lutego 2009 r., Irlandia/Parlament i Rada (C-301/06, EU:C:2009:68, pkt 90 i 91) Trybunał orzekł, że rozważań zawartych w wyroku PNR nie można odnieść do przetwarzania danych, o którym mowa w dyrektywie 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. 2006, L 105, s. 54). Trybunał uzasadnił ten wniosek okolicznością, że dyrektywa 2006/24, w odróżnieniu od decyzji rozpatrywanej w wyroku PNR, reguluje wyłącznie działalność dostawców usług na rynku wewnętrznym, natomiast nie reguluje działań władz publicznych w celach prawnokarnych. Wydaje się, że poprzez to rozumowanie Trybunał potwierdził (a contrario), iż wniosek wywiedziony w wyroku PNR można byłoby odnieść do przepisów dotyczących dostępu do zatrzymanych danych lub do ich wykorzystania przez te władze.

94 Wyrok Tele2 Sverige (pkt 67–81).

95 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. 2002, L 201, s. 37 – wyd. spec. w jęz. polskim, rozdz. 13, t. 29, s. 514).

bezpieczeństwa narodowego – są objęte zakresem stosowania tej dyrektywy, a co za tym idzie, zakresem stosowania karty. Zdaniem Trybunału ani przepisy dotyczące zatrzymywania danych, ani te dotyczące dostępu do zatrzymanych danych, nie są objęte wyłączeniem z zakresu stosowania tej dyrektywy zawartym w jej art. 1 ust. 3, który odnosi się między innymi do działalności państwa w dziedzinie ścigania karnego i ochrony bezpieczeństwa narodowego⁹⁶. Trybunał potwierdził tę linię orzecznictwą w wyroku *Ministerio Fiscal*⁹⁷.

216. Jednakże art. 702 FISA różni się od tego rodzaju uregulowań tym, że przepis ten nie nakłada na dostawców usług łączności elektronicznej obowiązku zatrzymywania danych ani przetwarzania ich w jakikolwiek inny sposób, jeżeli organy wywiadu nie wystąpią z wnioskiem o udzielenie dostępu do danych.

217. W związku z tym powstaje pytanie, czy uregulowania krajowe, które nakładają na tych dostawców obowiązek udostępniania danych organom publicznym do celów bezpieczeństwa narodowego, *niezależnie od obowiązku zatrzymywania danych*⁹⁸, są objęte zakresem stosowania RODO, a tym samym także zakresem stosowania karty.

218. *Pierwsze stanowisko* mogłoby sprowadzać się do pogodzenia (na tyle, na ile jest to możliwe) dwóch wskazanych wyżej linii orzecznictwa, poprzez interpretację wywiedzionego przez Trybunał w wyrokach *Tele2 Sverige* i *Ministerio Fiscal* wniosku dotyczącego stosowania prawa Unii do aktów prawnych regulujących dostęp organów krajowych do danych między innymi w celach ochrony bezpieczeństwa narodowego⁹⁹ w ten sposób, że ów wniosek ma zastosowanie wyłącznie w sytuacji, gdy dane były zatrzymywane *na podstawie obowiązku ustawowego* nałożonego w związku z art. 15 ust. 1 dyrektywy 2002/58. Wniosek ten nie miałby natomiast zastosowania w odmiennym stanie faktycznym wyroku PNR, który dotyczył przekazywania amerykańskiemu organowi właściwemu w sprawach bezpieczeństwa wewnętrznego danych zatrzymywanych przez przewoźników lotniczych z ich własnej woli w celach komercyjnych.

219. Zgodnie z *drugim podejściem*, które popiera Komisja i które uważam za bardziej przekonujące, rozumowanie zastosowane w wyrokach *Tele2 Sverige* i *Ministerio Fiscal* uzasadnia stosowanie prawa Unii do przepisów krajowych nakładających na dostawców usług łączności elektronicznej obowiązek udzielania wsparcia organom odpowiedzialnym za bezpieczeństwo narodowe, tak by mogły one uzyskać dostęp do niektórych danych, *niezależnie od tego, czy przepisy te obejmują obowiązek uprzedniego zatrzymania danych*.

96 Ponieważ dyrektywa 2002/58 konkretyzuje wymogi dyrektywy 95/46, uchylonej obecnie przez RODO, które w znacznej mierze powtarza jej treść, orzecznictwo dotyczące wykładni art. 1 ust. 3 dyrektywy 2002/58 ma, jak się wydaje, zastosowanie w drodze analogii do wykładni art. 2 ust. 2 RODO. Zobacz podobnie wyroki *Tele2 Sverige* (pkt 69) i *Ministerio Fiscal* (pkt 32).

97 Wyrok *Ministerio Fiscal* (pkt 34, 35 i 37).

98 To samo pytanie zostało zadane w kontekście trzech innych odesłań prejudycjalnych w sprawach toczących się przed Trybunałem. Zobacz sprawę C-623/17, *Privacy International* (Dz.U. 2018, C 22, s. 29) oraz sprawy połączone C-511/18 i C-512/18, *La Quadrature du Net* i in. i *French Data Network* i in. (Dz.U. 2018, C 392, s. 7).

99 Mimo że w wyroku *Tele2 Sverige* Trybunał skupił się na badaniu, czy ingerencje wynikające z rozpatrywanych przepisów dotyczących zatrzymywania danych i dostępu do nich są uzasadnione ze względu na cel, jakim jest zwalczanie przestępczości, to wniosek, do którego doszedł, odnosi się również, *mutatis mutandis*, do sytuacji, gdy celem, jakiemu służą te przepisy, jest ochrona bezpieczeństwa narodowego. Artykuł 15 ust. 1 dyrektywy 2002/58 wymienia bowiem wśród celów mogących stanowić uzasadnienie dla takich przepisów zarówno zwalczanie przestępczości, jak i ochronę bezpieczeństwa narodowego. Poza tym, art. 1 ust. 3 dyrektywy 2002/58 i art. 2 ust. 2 RODO wyłączają z zakresu stosowania tych aktów prawnych działalność państwa zarówno w dziedzinie bezpieczeństwa narodowego, jak i w obszarze prawa karnego. Zresztą przepisy rozpatrywane w sprawie, w której zapadł wyrok *Tele2 Sverige*, służyły również celowi związanemu z bezpieczeństwem narodowym. W pkt 119 tego wyroku Trybunał odniósł się bezpośrednio do problematyki uzasadnienia przepisów dotyczących zatrzymywania i dostępu do danych o ruchu i danych o lokalizacji, ze względu na cel, jakim jest ochrona bezpieczeństwa narodowego, który to cel obejmuje zwalczanie terroryzmu.

220. Istotą tego rozumowania nie jest bowiem przedmiot rozpatrywanych przepisów (jak w wyroku PNR), lecz okoliczność, że przepisy te regulowały działalność dostawców nakazując im podejmowanie czynności w zakresie przetwarzania danych. Taka działalność nie była działalnością państwa w dziedzinach wskazanych w art. 1 ust. 3 dyrektywy 2002/58 i w art. 3 ust. 2 dyrektywy 95/46, których treść została zasadniczo powtórzona w art. 2 ust. 2 RODO.

221. I tak, w wyroku *Tele2 Sverige* Trybunał zauważył, że „obowiązek zapewnienia [...] dostępu do danych zatrzymanych przez dostawców, dotyczy przetwarzania *przez nich* danych osobowych, które to przetwarzanie jest objęte zakresem stosowania tej dyrektywy”¹⁰⁰. Podobnie w wyroku *Ministerio Fiscal* Trybunał orzekł, że akty prawne nakładające na dostawców obowiązek udzielenia właściwym organom dostępu do zatrzymanych danych osobowych „wymagają przetwarzania wspomnianych danych *przez tych dostawców*”¹⁰¹.

222. Udostępnienie danych przez administratora organowi publicznemu odpowiada zaś definicji przetwarzania zawartej w art. 4 pkt 2 RODO¹⁰². To samo dotyczy uprzedniego filtrowania danych przy użyciu kryteriów wyszukiwania w celu wyodrębnienia danych, do których organy publiczne żądają dostępu¹⁰³.

223. Wniosuję z tego, że, zgodnie z rozumowaniem zastosowanym przez Trybunał w wyrokach *Tele2 Sverige* i *Ministerio Fiscal*, RODO, a więc i karta, mają zastosowanie do przepisów krajowych nakładających na dostawców usług łączności elektronicznej obowiązek udzielenia wsparcia organom odpowiedzialnym za bezpieczeństwo narodowe poprzez udostępnienie im danych, w razie potrzeby po ich przefiltrowaniu, niezależnie nawet od tego, czy istnieje jakikolwiek ustawowy obowiązek zatrzymywania tych danych.

224. Ponadto wykładnia taka zdaje się wynikać, przynajmniej pośrednio, z wyroku *Schrems*. Jak podkreślili DPC, rządy austriacki i polski oraz Komisja, Trybunał, badając ważność decyzji w sprawie bezpiecznej przystani, orzekł w tym wyroku, że prawo państwa trzeciego, którego dotyczy decyzja stwierdzająca odpowiedni stopień ochrony, powinno przewidywać (w celu ochrony przed ingerencjami jego organów publicznych w prawa podstawowe osób, których dane dotyczą, motywowanymi względami bezpieczeństwa narodowego), zabezpieczenia równoważne pod względem merytorycznym z tymi, które wynikają między innymi z art. 7, 8 i 47 karty¹⁰⁴.

225. Ścisłej rzecz ujmując wynika z tego, że przepis krajowy nakazujący dostawcom usług łączności elektronicznej spełnić pochodzące od organów właściwych w sprawach bezpieczeństwa narodowego żądanie dostępu do niektórych danych zatrzymywanych przez tych dostawców w ramach ich działalności komercyjnej, niezależnie od jakichkolwiek obowiązków ustawowych, identyfikując uprzednio żądane dane przy użyciu selektorów (jak to ma miejsce w ramach programu PRISM), nie wchodzi w zakres stosowania art. 2 ust. 2 RODO. Taki przepis nie dotyczy bowiem działalności państwa w dziedzinie bezpieczeństwa narodowego, lecz *działalności dostawców*, która jest objęta zakresem stosowania tego rozporządzenia. Podobnie byłoby w przypadku przepisu krajowego

100 Wyrok *Tele2 Sverige* (pkt 78, wyróżnienie moje). Użycie zwrotu „ponadto” świadczy o tym, że Trybunał, podkreślając w pkt 79 tego wyroku nierozzerwalny związek między obowiązkiem zatrzymywania danych rozpatrywanych w sprawie, w której zapadł ten wyrok, a przepisami odnoszącymi się do dostępu organów państwowych do zatrzymywanych danych, zamierzał wyłącznie potwierdzić swój wniosek dotyczący możliwości stosowania dyrektywy 2002/58.

101 Wyrok *Ministerio Fiscal* (pkt 37, wyróżnienie moje).

102 Zobacz podobnie wyrok *Ministerio Fiscal* (pkt 38).

103 Zobacz podobnie wyrok z dnia 13 maja 2014 r., *Google Spain i Google* (C-131/12, EU:C:2014:317, pkt 28).

104 Wyrok *Schrems* (pkt 91–96). W motywach 90, 124 i 141 decyzji w sprawie *Tarczy Prywatności* Komisja powołuje się zresztą na postanowienia karty, akceptując tym samym zasadę, zgodnie z którą ograniczenia praw podstawowych służące celom ochrony bezpieczeństwa narodowego powinny być zgodne z kartą.

nakładającego na przedsiębiorstwa wykorzystujące telekomunikacyjną „infrastrukturę szkieletową” wymóg udzielania organom odpowiedzialnym za bezpieczeństwo narodowe dostępu do danych będących „w tranzycie” za pośrednictwem wykorzystywanej przez te przedsiębiorstwa infrastruktury (jak ma to miejsce w ramach programu Upstream).

226. Natomiast gdy dane te znajdują się już w posiadaniu organów państwowych, ich przechowywanie i późniejsze wykorzystanie przez te organy do celów bezpieczeństwa narodowego jest moim zdaniem (z tych samych względów co wymienione w pkt 211 niniejszej opinii), objęte wyłączeniem przewidzianym w art. 2 ust. 2 RODO, w związku z czym nie wchodzi w zakres stosowania tego rozporządzenia, i, co za tym idzie, karty.

227. Podsumowując powyższe stwierdzam, że kontrola ważności decyzji w sprawie Tarczy Prywatności, w związku z ograniczeniami odnoszącymi się do wyrażonych w niej zasad mogącymi wynikać z działalności amerykańskich organów wywiadu, wymaga przeprowadzenia dwojakiego rodzaju weryfikacji.

228. *Po pierwsze*, należy zbadać, czy Stany Zjednoczone zapewniają stopień ochrony równoważny pod względem merytorycznym temu, który wynika z przepisów RODO i karty, w odniesieniu do ograniczeń będących skutkiem stosowania art. 702 FISA, na mocy którego to przepisu NSA przysługuje możliwość zobowiązania dostawców do udostępniania danych osobowych amerykańskim organom odpowiedzialnym za bezpieczeństwo narodowe.

229. *Po drugie*, postanowienia EKPC stanowią właściwe ramy odniesienia na potrzeby oceny, czy ograniczenia, jakimi mogłoby skutkować wdrożenie EO 12333, który to akt upoważnia organy wywiadu do samodzielnego (bez wsparcia podmiotów prywatnych) zbierania danych osobowych, podważają adekwatność stopnia ochrony zapewnianego przez Stany Zjednoczone. Postanowienia EKPC dostarczają również standardów porównawczych umożliwiających dokonanie oceny adekwatności tego stopnia ochrony w kontekście zatrzymywania i wykorzystania danych pozyskanych przez te organy do celów bezpieczeństwa narodowego.

230. Jednakże należy jeszcze ustalić, czy stwierdzenie adekwatności stopnia ochrony wiąże się z przyjęciem założenia, gromadzeniu danych na podstawie EO 12333 powinny towarzyszyć poziom zabezpieczenia równoważny pod względem merytorycznym z tymi, który powinien być zapewniony w Unii, *nawet w sytuacjach, gdy do ich gromadzenia dochodzi poza terytorium Stanów Zjednoczonych*, na etapie tranzytu danych z Unii do tego państwa trzeciego.

2) W przedmiocie konieczności zapewnienia odpowiedniego stopnia ochrony na etapie tranzytu danych

231. Przed Trybunałem prezentowane były trzy różne stanowiska odnoszące się do kwestii, czy konieczne jest, aby Komisja, oceniając adekwatność stopnia ochrony, jaki na etapie tranzytu danych z Unii na to terytorium zapewnia państwo trzecie, uwzględniała krajowe akty prawne dotyczące dostępu organów tego państwa do danych poza jego terytorium.

232. Po pierwsze, Facebook Ireland oraz rządy Stanów Zjednoczonych i Zjednoczonego Królestwa twierdzą zasadniczo, że istnienie takich aktów prawnych nie ma wpływu na ustalenia dotyczące adekwatności. W uzasadnieniu tego stanowiska podnoszą oni, że państwo trzecie nie ma możliwości kontrolowania wszystkich położonych poza jego terytorium kanałów komunikacji, którymi przesyłane są dane pochodzące z Unii, w związku z czym z założenia nigdy nie można byłoby zagwarantować, że inne państwo trzecie nie zbiera potajemnie danych w trakcie ich tranzytu.

233. Po drugie, DPC, M. Schrems, EPIC, rządy austriacki i niderlandzki, Parlament i EROD podnoszą, że z ustanowionego w art. 44 RODO wymogu ciągłości stopnia ochrony wynika, iż stopień ochrony powinien być odpowiedni w ciągu całego procesu przekazywania danych, w tym również w czasie, gdy są one przesyłane podmorskimi kablami zanim dotrą na terytorium docelowego państwa trzeciego.

234. Po trzecie, Komisja uznając tę zasadę podnosi, że stwierdzenie adekwatności odnosi się wyłącznie do ochrony zapewnianej przez dane państwo trzecie *w jego granicach*, w związku z czym okoliczność, iż odpowiedni stopień ochrony nie jest gwarantowany *podczas tranzytu* danych do tego państwa trzeciego, nie podważa ważności decyzji stwierdzającej odpowiedni stopień ochrony. Poza tym administrator ma jednak zgodnie z art. 32 RODO obowiązek zapewnić bezpieczeństwo przekazywanych danych osobowych, chroniąc je w najwyższym możliwym stopniu na etapie ich tranzytu do rzeczonoego państwa trzeciego.

235. W tym względzie pragnę zauważyć, że w art. 44 RODO przekazywanie danych do państwa trzeciego uzależnione zostało od spełnienia warunków ustanowionych na mocy przepisów rozdziału V tego rozporządzenia, jeżeli dane „po przekazaniu” mają być przetwarzane. Znaczenie tego zwrotu można rozumieć bądź w taki sposób, za jakim opowiedział się rząd Stanów Zjednoczonych w udzielonej przezeń na piśmie odpowiedzi na pytania Trybunału, to znaczy, że warunki te powinny być spełnione, *gdy dane dotrą już do miejsca docelowego*, bądź też, że obowiązują one *od momentu, gdy to przekazywanie zostało zainicjowane* (w tym na etapie tranzytu).

236. Ponieważ brzmienie art. 44 RODO nie jest jednoznaczne, wykładnia celowościowa skłania mnie do przyjęcia drugiej z powyższych interpretacji, a zatem – do poparcia drugiego z powyższych stanowisk. Gdyby bowiem uznać, że przewidziany w tym przepisie wymóg ciągłości stopnia ochrony odnosi się wyłącznie do mechanizmów nadzoru stosowanych w ramach terytorium docelowego państwa trzeciego, przepis ten mógłby być obchodzony w sytuacjach, gdy to państwo trzecie stosuje takie mechanizmy inwigilacji poza swoim terytorium, na etapie tranzytu danych. Aby uniknąć tego ryzyka, ocena adekwatności stopnia ochrony, jaki zapewnia państwo trzecie, powinna dotyczyć ogółu przepisów przewidzianych w porządku prawnym tego państwa trzeciego¹⁰⁵ (w szczególności w dziedzinie bezpieczeństwa narodowego), wśród których znajdują się zarówno te odnoszące się do nadzoru stosowanego na jego terytorium, jak i te umożliwiające nadzór danych w trakcie ich tranzytu na to terytorium¹⁰⁶.

237. Niezależnie od powyższego, nikt nie kwestionuje tego, że (co podkreśliła EROD) ocena adekwatności stopnia ochrony dotyczy wyłącznie – jak wynika z art. 45 ust. 1 RODO – przepisów należących do porządku prawnego *docelowego państwa trzeciego, do którego przekazywane są dane*. Na ocenę tę nie ma wpływu wskazywany przez Facebook Ireland oraz rządy Stanów Zjednoczonych i Zjednoczonego Królestwa brak możliwości zapewnienia, że państwo trzecie nie będzie potajemnie zbierało danych podczas ich tranzytu. Ponadto takiego ryzyka nie można wykluczyć nawet wówczas, gdy dane już dotrą na terytorium docelowego państwa trzeciego.

238. Poza tym prawdą jest również, że Komisja, oceniając adekwatność stopnia ochrony, jaki zapewnia państwo trzecie, mogłaby zetknąć się z przypadkiem zaniechania ujawnienia jej przez to państwo trzecie istnienia niektórych tajnych programów nadzoru. Nie oznacza to jednak, że Komisja, *gdy poweźmie wiedzę o takich programach*, może ich nie uwzględniać w ramach oceny stopnia ochrony, jaki zapewnia to państwo trzecie. Podobnie w sytuacji gdy, po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony, Komisji zostanie ujawnione istnienie pewnych tajnych programów

¹⁰⁵ Zobacz podobnie wyrok Schrems (pkt 74 i 75).

¹⁰⁶ Zobacz podobnie EROD, EU-US Privacy Shield – Second Annual Joint Review, z dnia 22 stycznia 2019 r. (s. 17, pkt 86).

nadzoru stosowanych przez dane państwo trzecie na jego terytorium lub podczas tranzytu danych na to terytorium, Komisja ma obowiązek ponownego przeanalizowania swojego ustalenia odnoszącego się do adekwatności stopnia ochrony, jaki zapewnia to państwo trzecie, w przypadku gdy tego rodzaju ujawnienie spowoduje powstanie wątpliwości w tym przedmiocie¹⁰⁷.

3) W przedmiocie uwzględnienia poczynionych przez Komisję i sąd odsyłający ustaleń faktycznych dotyczących prawa Stanów Zjednoczonych

239. Mimo że bezsporne jest, iż Trybunał nie jest właściwy do dokonywania wykładni prawa państwa trzeciego, która byłaby wiążąca w porządku prawnym tego państwa, to ważność decyzji w sprawie Tarczy Prywatności zależy od zasadności dokonanych przez Komisję ocen dotyczących stopnia ochrony praw podstawowych osób, których dane są przekazywane do Stanów Zjednoczonych, jaki jest zapewniany w oparciu o obowiązujące w tym państwie trzecim przepisy prawa i praktykę. Komisja miała bowiem obowiązek uzasadnienia stwierdzenia dotyczącego adekwatności odnosząc się do czynników wymienionych w art. 45 ust. 2 RODO, który dotyczy między innymi treści prawa rzeczonego państwa trzeciego¹⁰⁸.

240. High Court (wysoki trybunał) w swoim wyroku z dnia 3 października 2017 r., po dokonaniu oceny przedłożonych przez strony postępowania dowodów, przedstawił szczegółowe ustalenia opisujące istotne aspekty amerykańskiego prawa¹⁰⁹. Omówienie to w dużej mierze pokrywa się z poczynionymi przez Komisję w decyzji w sprawie Tarczy Prywatności ustaleniami dotyczącymi treści zasad regulujących zbieranie i udostępnianie amerykańskim organom wywiadu przekazanych danych oraz środków ochrony prawnej i mechanizmów sprawowania kontroli nad tą działalnością.

241. Sąd odsyłający oraz kilka zainteresowanych stron, które przedłożyły Trybunałowi uwagi, w większym stopniu kwestionują skutki prawne, jakie Komisja wywiodła z tych ustaleń – a mianowicie wnioszek, zgodnie z którym Stany Zjednoczone zapewniają odpowiedni stopień ochrony praw podstawowych osób, których dane są przekazywane na podstawie tej decyzji – niż przedstawione przez nią omówienie treści amerykańskiego prawa.

242. W związku z powyższym dokonam oceny ważności decyzji w sprawie Tarczy Prywatności głównie w świetle poczynionych przez samą Komisję ustaleń dotyczących treści prawa amerykańskiego, badając, czy ustalenia te uzasadniają przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony.

243. W tym względzie nie podzielam stanowiska reprezentowanego przez DPC i M. Schremsa, zgodnie z którym ustalenia High Court (wysokiego trybunału) na temat prawa Stanów Zjednoczonych są wiążące dla Trybunału w ramach badania ważności decyzji w sprawie Tarczy Prywatności. Twierdzą oni, że skoro prawo obce, zgodnie z irlandzkim prawem procesowym, stanowi element stanu faktycznego, wyłącznie sąd odsyłający jest właściwy do ustalenia jego treści.

244. Wprawdzie w utrwalonym orzecznictwie przyznano sądom krajowym wyłączną kompetencję do ustalania istotnych okoliczności faktycznych oraz dokonywania wykładni prawa państwa członkowskiego i stosowania tego prawa w rozpoznawanym przezeń sporze¹¹⁰. Orzecznictwo to stanowi wyraz podziału między Trybunał a sąd odsyłający funkcji pełnionych przez te sądy w ramach

¹⁰⁷ Zobacz art. 45 ust. 5 RODO. Zobacz również wyrok Schrems (pkt 76).

¹⁰⁸ Decyzja w sprawie bezpiecznej przystani została uznana za nieważną, ponieważ Komisja nie wykazała w tej decyzji, że Stany Zjednoczone rzeczywiście zapewniają odpowiedni stopień ochrony poprzez swoje ustawodawstwo lub zobowiązania międzynarodowe (wyrok Schrems, pkt 97). W szczególności Komisja nie stwierdziła istnienia ani reguł ogólnopaństwowych służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób, których dane dotyczą (wyrok Schrems, pkt 88), ani skutecznej ochrony prawnej przed ingerencją tego rodzaju (wyrok Schrems, pkt 89).

¹⁰⁹ Streszczenie tych ustaleń znajduje się w pkt 54–73 niniejszej opinii.

¹¹⁰ Zobacz m.in. wyroki z dnia 4 maja 1999 r., Sürül (C-262/96, EU:C:1999:228, pkt 95); z dnia 11 września 2008 r., Eckelkamp i in. (C-11/07, EU:C:2008:489, pkt 32); z dnia 26 października 2016 r., Senior Home (C-195/15, EU:C:2016:804, pkt 20).

postępowania ustanowionego na mocy art. 267 TFUE. Podczas gdy Trybunał jest wyłącznie właściwy do dokonywania wykładni prawa Unii i orzekania co do ważności prawa wtórnego, zadaniem sądu krajowego rozpoznającego zawisły przed nim konkretny spór jest ustalenie stanu faktycznego i prawnego, tak aby Trybunał mógł udzielić mu użytecznej odpowiedzi.

245. Nie wydaje mi się, aby ta wyłączna kompetencja przysługująca sądowi odsyłającemu mogła być odniesiona do ustalania treści prawa państwa trzeciego jako okoliczności, która może mieć wpływ na wniosek Trybunału co do ważności aktu prawa wtórnego¹¹¹. Skoro stwierdzenie nieważności takiego aktu wywiera skutki erga omnes w porządku prawnym Unii¹¹², wniosek wydany przez Trybunał nie może być zależny od tego, skąd pochodzi odesłanie prejudycjalne. Jak podkreślili Facebook Ireland i rząd Stanów Zjednoczonych, gdyby Trybunał był związany ustaleniami sądu odsyłającego dotyczącymi prawa państwa trzeciego, wniosek taki byłby zależny od tego, skąd pochodzi pytanie prejudycjalne, ponieważ ustalenia te mogłyby różnić się w zależności od sądu krajowego, który je poczynił.

246. Z powyższych względów uważam, że w sytuacji, gdy udzielenie odpowiedzi na pytanie prejudycjalne dotyczące ważności aktu prawnego Unii wymaga dokonania oceny treści prawa państwa trzeciego, Trybunał może co prawda uwzględnić ustalenia sądu odsyłającego dotyczące tego prawa, jednakże nie jest nimi związany. Trybunał może w razie potrzeby pominąć te ustalenia lub uzupełnić je biorąc pod uwagę (zgodnie z zasadą kontradyktoryjności) inne źródła w celu ustalenia okoliczności niezbędnych dla oceny ważności rozpatrywanego aktu prawnego¹¹³.

4) W przedmiocie znaczenia standardu „merytorycznej równoważności”

247. Przypomnę, że ważność decyzji w sprawie Tarczy Prywatności zależy od ustalenia, czy w porządku prawnym Stanów Zjednoczonych zapewniony jest – na rzecz osób, których dane są przekazywane z Unii do tego państwa trzeciego – stopień ochrony przed ingerencją w korzystanie przez nie z praw podstawowych „równoważny pod względem merytorycznym” z tym, jaki jest zapewniony w państwach członkowskich na mocy RODO i karty oraz (w dziedzinach wyłączonych z zakresu stosowania prawa Unii) na mocy ich zobowiązań wynikających z EKPC.

248. Jak zaznaczył Trybunał w wyroku Schrems¹¹⁴, standard ten nie oznacza, że stopień ochrony powinien być „identyczny” z tym, jaki jest wymagany w Unii. Mimo że środki, z jakich to państwo trzecie korzysta w celu zapewnienia ochrony praw osób, których dane dotyczą, mogą różnić się od środków, jakie przewiduje RODO w związku z kartą, to jednak „środki te powinny w praktyce skutecznie zapewniać ochronę merytorycznie równoważną ochronie gwarantowanej w Unii”.

249. Moim zdaniem wynika z tego również, że prawo docelowego państwa trzeciego może odzwierciedlać swój własny system wartości, zgodnie z którym waga poszczególnych wchodzących w grę interesów może różnić się od wagi, jaka jest im przypisywana w porządku prawnym Unii. Poza tym ochrona danych osobowych obowiązująca w Unii spełnia szczególnie wysokie standardy w porównaniu ze stopniem ochrony, jaki obowiązuje w pozostałych częściach świata. Kryterium „merytorycznej równoważności” należy według mnie stosować w taki sposób, aby zachować pewną

111 Zobacz w tym względzie wyrok Supreme Court (sądu najwyższego) z dnia 31 maja 2019 r. (pkt 6.18).

112 Zobacz wyrok z dnia 13 maja 1981 r., International Chemical Corporation (66/80, EU:C:1981:102, pkt 12 i 13).

113 Zobacz w tym względzie wyrok z dnia 22 marca 2012 r., GLS (C-338/10, EU:C:2012:158, pkt 15, 33 i 34), w którym Trybunał, oceniając ważność rozporządzenia nakładającego cło antydumpingowe, uwzględnił przedłożone przez Komisję na jego żądanie statystyki Eurostatu. Zobacz również wyrok z dnia 22 października 1991 r., Nölle (C-16/90, EU:C:1991:402, pkt 17, 23 i 24). Podobnie w wyroku Schrems (pkt 90) Trybunał, badając ważność decyzji w sprawie bezpiecznej przystani, uwzględnił pewne komunikaty Komisji.

114 Wyrok Schrems (pkt 73 i 74).

elastyczność, uwzględniając różne tradycje prawne i kulturowe. Jeżeli jednak kryterium to ma nie być pozbawione swej treści, niezbędne jest, aby pewne minimalne zabezpieczenia i ogólne wymogi ochrony praw podstawowych wynikające z RODO, karty i EKPC miały swoje odpowiedniki w porządku prawnym docelowego państwa trzeciego¹¹⁵.

250. W tym względzie, zgodnie z art. 52 ust. 1 karty, wszelkie ograniczenia w korzystaniu z uznanych w niej praw i wolności muszą być przewidziane ustawą i szanować istotę tych praw i wolności oraz, zgodnie z zasadą proporcjonalności, mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Wymogi te stanowią co do zasady odpowiednik tych, które zostały wyrażone w art. 8 ust. 2 EKPC¹¹⁶.

251. Zgodnie z art. 52 ust. 3 karty w zakresie, w jakim prawa gwarantowane przez nią w art. 7, 8 i 47 odpowiadają prawom zagwarantowanym w art. 8 i 13 EKPC, znaczenie i zakres tych praw są takie same, przy czym przyjmuje się, że w prawie Unii może zostać przyznana dalej idącą ochronę. Z tego punktu widzenia, co zostanie wykazane w mojej analizie, standardy wynikające z art. 7, 8 i 47 karty, zgodnie z ich wykładnią dokonaną przez Trybunał, są pod pewnymi względami bardziej rygorystyczne niż te, które wynikają z art. 8 EKPC, zgodnie z jego wykładnią dokonaną przez Europejski Trybunał Praw Człowieka (zwany dalej „ETPC”).

252. Zwracam również uwagę, że toczące się przed każdym z tych sądów sprawy stanowią dla nich sposobność zrewidowania niektórych aspektów ich orzecznictwa. I tak, po pierwsze, dwa niedawne wyroki ETPC dotyczące kontroli komunikatów elektronicznych – a mianowicie wyroki *Centrum för Rättvisa* przeciwko Szwecji¹¹⁷ i *Big Brother Watch* przeciwko Zjednoczonemu Królestwu¹¹⁸ – zostały przekazane do ponownego rozpoznania przez wielką izbę. Po drugie, trzy sądy krajowe zwróciły się do Trybunału z odesłaniami prejudycjalnymi, które otwierają dyskusję na temat potrzeby zmodyfikowania kierunku jego orzecznictwa zapoczątkowanego wyrokiem *Tele2 Sverige*¹¹⁹.

253. Wyjaśniwszy powyższe, przeanalizuję teraz kwestię ważności decyzji w sprawie *Tarczy Prywatności* w świetle art. 45 ust. 1 RODO w związku z kartą i EKPC, które zapewniają, po pierwsze, prawo do poszanowania życia prywatnego i ochrony danych osobowych [część b)], a po drugie, skuteczną ochronę sądową [część c)].

b) W przedmiocie ważności decyzji w sprawie Tarczy Prywatności w świetle prawa do poszanowania życia prywatnego i do ochrony danych osobowych

254. W pytaniu czwartym sąd odsyłający w istocie kwestionuje merytoryczną równowagę między stopniem ochrony, jaki zapewniają Stany Zjednoczone, a stopniem ochrony przysługującym w Unii osobom, których dane dotyczą, na podstawie praw podstawowych, jakimi są prawo do poszanowania życia prywatnego i ochrony danych osobowych.

¹¹⁵ Zobacz podobnie, grupa robocza z art. 29, *Adequacy Referential* (updated), 28 listopada 2017 r., WP 254 (s. 3, 4 i 9).

¹¹⁶ Artykuł 8 ust. 2 EKPC nie odwołuje się jednakże do pojęcia „istoty” prawa do poszanowania życia prywatnego. Zobacz na ten temat przypis 161 do niniejszej opinii.

¹¹⁷ Wyrok ETPC z dnia 19 czerwca 2018 r. (CE:ECHR:2018:0619JUD003525208, zwany dalej „wyrokiem *Centrum för Rättvisa*”).

¹¹⁸ Wyrok ETPC z dnia 13 września 2018 r. (CE:ECHR:2018:0913JUD005817013, zwany dalej „wyrokiem *Big Brother Watch*”).

¹¹⁹ Zobacz sprawy wymienione w przypisie 98 do niniejszej opinii oraz sprawę C-520/18, *Ordre des barreaux francophones et germanophones* i in. (Dz.U. 2018, C 408, s. 39).

1) W przedmiocie istnienia ingerencji

255. W motywach 67–124 decyzji w sprawie Tarczy Prywatności Komisja wskazała, że istnieje możliwość, iż amerykańskie organy publiczne mają dostęp do danych przekazywanych z Unii i wykorzystują te dane do celów bezpieczeństwa narodowego w ramach programów opartych między innymi na art. 702 FISA lub EO 12333.

256. Wdrożenie tych programów pociąga za sobą ingerencje ze strony amerykańskich służb wywiadowczych, które – w sytuacji gdyby dochodziło do nich za sprawą organów państwa członkowskiego – byłyby uznane za ingerencje w korzystanie z prawa do poszanowania życia prywatnego gwarantowanego przez art. 7 karty i art. 8 EKPC. Wdrożenie tych programów naraża również osoby, których dane dotyczą, na ryzyko, że ich dane osobowe będą podlegały przetwarzaniu niezgodnemu z wymogami ustanowionymi w art. 8 karty¹²⁰.

257. Wyjaśnię na wstępie, że prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych obejmują nie tylko ochronę treści komunikatów, lecz także dane o ruchu¹²¹ i dane dotyczące lokalizacji (określane łącznie pojęciem „metadanych”). Zarówno Trybunał jak i ETPC przyznały bowiem, że metadane, podobnie jak dane dotyczące treści, mogą dostarczać bardzo precyzyjnych wskazówek dotyczących życia prywatnego danej osoby¹²².

258. Zgodnie z orzecznictwem Trybunału, przy ustalaniu, czy doszło do ingerencji w korzystanie z gwarantowanego w art. 7 karty prawa podstawowego, nie ma znaczenia to, czy określone dane mają charakter wrażliwy ani też to, czy zainteresowane osoby doświadczyły ewentualnych niedogodności ze względu na zastosowanie rozpatrywanego mechanizmu nadzoru¹²³.

259. Przypomniawszy powyższe należy wskazać, że programy nadzoru oparte na art. 702 FISA skutkują przede wszystkim ingerencjami w korzystanie z praw podstawowych przez osoby, których komunikaty pasują do selektorów wybranych przez NSA i w związku z tym są przekazywane do tej agencji przez dostawców usług łączności elektronicznej¹²⁴. Ściślej rzecz ujmując, spoczywający na dostawcach obowiązek *udostępnienia* danych NSA w zakresie, w jakim stanowi odstępstwo od zasady poufności komunikacji¹²⁵, stanowi sam w sobie ingerencję, nawet jeśli dane te nie byłyby następnie przeglądane lub wykorzystywane przez organy wywiadu¹²⁶. *Zatrzymywanie* i faktyczny *dostęp* tych organów do metadanych i do treści udostępnionych im komunikatów, podobnie jak *wykorzystanie* tych danych stanowią kolejne ingerencje¹²⁷.

120 Mimo że przetwarzanie może naruszać jednocześnie art. 7 i 8 karty, właściwe ramy analizy na potrzeby stosowania art. 8 różnią się pod względem struktury od tych, które odnoszą się do art. 7. Prawo do ochrony danych osobowych, zgodnie z art. 8 ust. 2 karty oznacza, że „[d]ane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą” oraz że „[k]ażdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.” Do naruszenia tego prawa dochodzi, gdy dane osobowe są poddawane przetwarzaniu niespełniającemu tych wymogów. Dzieje się tak między innymi w sytuacji, gdy przetwarzanie nie odbywa się ani za zgodą osoby, której dane dotyczą, ani na innej uzasadnionej podstawie przewidzianej ustawą. W tego rodzaju sytuacji, mimo że kwestia istnienia ingerencji i kwestia jej uzasadnienia są odrębne pod względem konceptualnym w ramach art. 7, kwestie te nakładają się na siebie, jeśli chodzi o art. 8 karty.

121 Artykuł 2 akapit drugi lit. b) dyrektywy 2002/58 definiuje pojęcie „danych o ruchu” jako „wszelkie dane przetwarzane do celów przekazywania komunikatu w sieci łączności elektronicznej lub naliczania opłat za te usługi”.

122 Zobacz wyrok z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in. (sprawy połączone C-293/12 i C-594/12, EU:C:2014:238, zwany dalej „wyrokiem Digital Rights Ireland”, pkt 27) oraz wyrok Tele2 Sverige (pkt 99). Zobacz również wyrok ETPC z dnia 2 sierpnia 1984 r., Malone przeciwko Zjednoczonemu Królestwu (CE:ECHR:1984:0802JUD000869179, § 84) i wyrok z dnia 8 lutego 2018 r., Ben Faiza przeciwko Francji (CE:ECHR:2018:0208JUD003144612, § 66).

123 Zobacz wyrok Digital Rights Ireland (pkt 33); opinia 1/15 (pkt 124); wyrok Ministerio Fiscal (pkt 51).

124 Zobacz motywy 78–81 oraz załącznik VI, pkt II decyzji w sprawie Tarczy Prywatności.

125 Zobacz w tym względzie wyrok Digital Rights Ireland (pkt 32).

126 Zobacz podobnie opinię 1/15 (pkt 124 i 125), z której wynika, że przekazanie danych osobie trzeciej stanowi ingerencję w korzystanie z praw podstawowych przysługujących osobom, których dane dotyczą, niezależnie od tego, w jaki sposób dane te zostaną następnie wykorzystane.

127 Zobacz podobnie wyrok Digital Rights Ireland (pkt 35); wyrok Schrems (pkt 87) i opinię 1/15 (pkt 123–126).

260. Co więcej, zgodnie z ustaleniami sądu odsyłającego¹²⁸ oraz z innymi źródłami takimi jak sprawozdanie PCLOB na temat programów wdrożonych na mocy art. 702 FISA, o którym Trybunał został poinformowany przez rząd amerykański¹²⁹, NSA w ramach programu Upstream posiada już, *na potrzeby filtrowania, dostęp* do obszernych zbiorów („pakietów”) danych uczestniczących w przepływie komunikatów przechodzących przez telekomunikacyjną „infrastrukturę szkieletową” i obejmujących komunikaty, które nie zawierają selektorów wskazanych przez NSA. NSA może analizować te zbiory danych wyłącznie w celu szybkiego ustalenia w sposób zautomatyzowany, czy zawierają one te selektory. W bazach danych NSA zapisywane są wówczas wyłącznie przefiltrowane w ten sposób dane. Ten dostęp do danych w celu ich filtrowania według mnie również stanowi ingerencję w korzystanie z prawa do poszanowania życia prywatnego przysługującego osobom, których dane dotyczą, niezależnie od sposobu późniejszego wykorzystania zatrzymanych danych¹³⁰.

261. Ponadto udostępnianie i filtrowanie rozpatrywanych danych¹³¹, dostęp organów wywiadu do tych danych, jak również ewentualne zezatrzymywanie, analizowanie, przechowywanie i wykorzystywanie rzeczonych danych wchodzi w zakres pojęcia „przetwarzania” w rozumieniu art. 4 pkt 2 RODO oraz art. 8 ust. 2 karty. W związku z tym takie przetwarzanie powinno spełniać wymogi przewidziane w tym ostatnim przepisie¹³².

262. Nadzór prowadzony na podstawie EO 12333 mógłby z kolei skutkować bezpośrednim dostępem organów wywiadu do danych w trakcie ich tranzytu, co powodowałoby ingerencję w zagwarantowane w art. 8 EKPC prawo. Kolejną ingerencję stanowiłoby ewentualne późniejsze wykorzystywanie tych danych.

2) Charakter ingerencji w świetle wymogu, aby były one „przewidziane ustawą”

263. W myśl orzecznictwa Trybunału¹³³ i ETPC¹³⁴ wymóg, aby wszelkie ingerencje w korzystanie z praw podstawowych były „przewidziane ustawą” (zgodnie z brzmieniem art. 52 ust. 1 karty i art. 8 ust. 2 EKPC) oznacza nie tylko, że akt prawny przewidujący ingerencję powinien mieć podstawę prawną w prawie wewnętrznym, lecz również, że ta podstawa prawna powinna posiadać pewne cechy, jeśli chodzi o dostępność i przewidywalność, tak aby uniknąć ryzyka arbitralności.

264. W tym względzie strony i zainteresowani, którzy przedłożyli Trybunałowi uwagi, mają zasadniczo przeciwne stanowiska co do kwestii, czy art. 702 FISA oraz EO 12333 spełniają warunek odnoszący się do przewidywalności prawa.

265. Warunek ten, zgodnie z jego wykładnią dokonaną przez Trybunał¹³⁵ i przez ETPC¹³⁶, jest spełniony, gdy uregulowania stanowiące ingerencję w korzystanie z prawa do poszanowania życia prywatnego zawierają jasne i precyzyjne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiają minimalne zabezpieczenia służące temu, aby osoby, których dane dotyczą,

128 Zobacz pkt 60 niniejszej opinii.

129 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA], 2 lipca 2014 r. (zwane dalej „sprawozdaniem PCLOB”, s. 84 i 111). Zobacz również grupa robocza z art. 29, EU-U.S. Privacy Shield – First Annual Joint Review, 28 listopada 2017 r., WP 255 (pkt B.1.1, s. 15).

130 Zobacz przypis 126 do niniejszej opinii.

131 Zobacz na ten temat pkt 222 niniejszej opinii.

132 Zobacz opinię 1/15 (pkt 123 i przytoczone tam orzecznictwo).

133 Zobacz w szczególności opinię 1/15 (pkt 146).

134 Zobacz w szczególności wyrok ETPC z dnia 2 sierpnia 1984 r., Malone przeciwko Zjednoczonemu Królestwu (CE:ECHR:1984:0802JUD000869179, § 66), rozstrzygnięcie z dnia 29 czerwca 2006 r., Weber i Saravia przeciwko Niemcom (CE:ECHR:2006:0629DEC005493400, zwany dalej „rozstrzygnięciem Weber i Saravia”, § 84 i przytoczone tam orzecznictwo.); wyrok z dnia 4 grudnia 2015 r., Zakharov przeciwko Rosji (CE:ECHR:2015:1204JUD004714306, zwany dalej „wyrokiem Zakharov”, § 228).

135 Zobacz w szczególności wyrok Digital Rights Ireland (pkt 54 i 65); wyrok Schrems (pkt 91); wyrok Tele2 Sverige (pkt 109); opinia 1/15 (pkt 141).

136 Zobacz w szczególności rozstrzygnięcie Weber i Saravia (§ 94 i 95); wyrok Zakharov (§ 236); i wyrok ETPC z dnia 12 stycznia 2016 r., Szabó i Vissy przeciwko Węgrom (CE:ECHR:2016:0112JUD003713814, zwany dalej „wyrokiem Szabó i Vissy”, § 59).

miały wystarczające gwarancje ochrony ich danych przed ryzykiem nadużyć oraz uzyskaniem do nich bezprawnego dostępu i ich wykorzystywaniem. Reguły te powinny w szczególności określać, w jakich okolicznościach i pod jakimi warunkami organy publiczne mogą przechowywać dane osobowe, uzyskiwać do nich dostęp i wykorzystywać je¹³⁷. Poza tym sama podstawa prawna, z której wynika możliwość ingerencji, powinna określać zakres ograniczenia w korzystaniu z prawa podstawowego do poszanowania życia prywatnego¹³⁸.

266. Podobnie jak M. Schrems i EPIC wątpię, czy EO 12333 oraz PPD 28, która ustanawia zabezpieczenia towarzyszące całej działalności wywiadowczej odnośnie do transmisji elektromagnetycznych¹³⁹, są dostatecznie przewidywalne, aby uznać, że mają „cechy ustawy”.

267. Z powyższych aktów prawnych jednoznacznie wynika, że nie ustanawiają one egzekwowalnych praw na rzecz osób, których dane dotyczą¹⁴⁰. Osoby te nie mogą zatem powoływać się przed sądami na zabezpieczenia przewidziane w PPD 28¹⁴¹. Komisja uznała zresztą w decyzji w sprawie Tarczy Prywatności, że, mimo iż zabezpieczenia przewidziane w tej dyrektywie prezydenckiej są wiążące dla służb wywiadowczych¹⁴², to „nie są sformułowane w języku prawniczym”¹⁴³. EO 12333 i PPD 28 należy raczej uznać za wewnętrzne instrukcje administracyjne, które mogą być odwoływane lub zmieniane przez prezydenta Stanów Zjednoczonych. Natomiast ETPC orzekał już, że wewnętrzne wytyczne administracyjne nie mają charakteru „ustawy”¹⁴⁴.

268. Jeśli chodzi o art. 702 FISA, przewidywalność tego przepisu jest kwestionowana przez M. Schremsa z tego powodu, że wyborowi kryteriów selekcji stosowanych do filtrowania danych nie towarzyszą dostateczne zabezpieczenia przeciwko ryzykom nadużyć. Ponieważ to zagadnienie łączy się również z kwestią dotyczącą ściśle niezbędnego charakteru ingerencji przewidzianych w art. 702 FISA, przeanalizuję je w dalszej części opinii¹⁴⁵.

269. Trzecie pytanie prejudycjalne pokrywa się z tematyką przestrzegania warunku odnoszącego się do „charakteru ustawowego”. Poprzez to pytanie sąd odsyłający chciałby w istocie ustalić, czy adekwatność stopnia ochrony, jaką zapewnia państwo trzecie, należy rozpatrywać wyłącznie w świetle prawnie wiążących zasad obowiązujących w tym państwie trzecim i praktyki mającej na celu zapewnienie ich przestrzegania, czy także w świetle innych, niewiążących instrumentów i mechanizmów kontroli pozasądowej stosowanych w tym państwie.

137 Zobacz wyrok Tele2 Sverige (pkt 117) i opinię 1/15 (pkt 190). Zobacz między innymi wyrok ETPC z dnia 2 sierpnia 1984 r., Malone przeciwko Zjednoczonemu Królestwu (CE:ECHR:1984:0802JUD000869179, § 67); wyrok Zakharov (§ 229); wyrok Szabó i Vissy (§ 62). ETPC wyjaśnia w tych wyrokach, że wymóg przewidywalności w przypadku przechwytywania komunikatów nie ma takiego samego znaczenia jak w innych dziedzinach. W kontekście tajnych mechanizmów nadzoru „wymóg przewidywalności nie może oznaczać, że należy umożliwić komukolwiek przewidywanie czy i kiedy jego komunikaty mogą być przechwytywane przez organy, tak aby w konsekwencji osoba ta mogła odpowiednio dostosować swoje zachowanie”.

138 Opinia 1/15 (pkt 139). Zobacz również podobnie wyrok ETPC z dnia 25 marca 1983 r., Silver i in. przeciwko Zjednoczonemu Królestwu (CE:ECHR:1983:0325JUD000594772, § 88 i 89).

139 Motywy 69–77 oraz załącznik VI pkt I decyzji w sprawie Tarczy Prywatności zawierają omówienie PPD 28. Wyjaśniono w nich, że ta prezydencka dyrektywa ma zastosowanie zarówno do działalności wywiadowczej prowadzonej na podstawie art. 702 FISA, jak i działalności prowadzonej poza terytorium Stanów Zjednoczonych.

140 Punkt 3.7 lit. c) EO 12333 stanowi: „[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person”. Artykuł 6 lit. d) PPD 28 stanowi również: „This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person”.

141 Zobacz podobnie EROD, EU-U.S. Privacy Shield – Second Annual Joint Review, z dnia 22 stycznia 2019 r. (pkt 99).

142 Zobacz motywy 69 i 77 decyzji w sprawie Tarczy Prywatności.

143 Motyw 76 decyzji w sprawie Tarczy Prywatności.

144 Zobacz wyrok ETPC z dnia 25 marca 1983 r., Silver i in. przeciwko Zjednoczonemu Królestwu (CE:ECHR:1983:0325JUD000594772, § 26 i 86).

145 Zobacz pkt 295–301 niniejszej opinii. W wyroku Tele2 Sverige (pkt 116 i 117) oraz w opinii 1/15 (pkt 140 i 141), warunek przewidywalności prawa został przedstawiony jako nierozdzielnie związany z warunkiem niezbędności i proporcjonalności ingerencji. Podobnie w orzecznictwie ETPC istnienie skutecznych zabezpieczeń przeciwko ryzykom nadużyć jest zarówno elementem warunku „przewidywalności” ingerencji, jak i warunku dotyczącego jej „niezbędności w społeczeństwie demokratycznym”, przy czym spełnienie tych dwóch warunków bada się łącznie. Zobacz między innymi wyrok ETPC z dnia 18 maja 2010 r., Kennedy przeciwko Zjednoczonemu Królestwu (CE:ECHR:2010:0518JUD002683905, § 155); wyrok Zakharov (§ 236); wyrok Centrum för Rättvisa (§ 107); wyrok Big Brother Watch (§ 322).

270. Artykuł 45 ust. 2 lit. a) RODO zawiera w tym względzie niewyczerpujące wyliczenie okoliczności, jakie Komisja powinna uwzględniać oceniając adekwatność stopnia ochrony zapewnianego w państwie trzecim. Wśród tych okoliczności znajduje się mające zastosowanie ustawodawstwo oraz sposób, w jaki jest ono wdrażane. W przepisie tym wyszczególniono również inne rodzaje norm, takie jak zasady dotyczące wykonywania zawodu i środki bezpieczeństwa. Poza tym, przepis ten wymaga również, aby uwzględniać „skuteczne i egzekwowalne prawa” oraz „prawa osób [...], których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia”¹⁴⁶.

271. Powyższy przepis, interpretowany całościowo i z uwzględnieniem faktu, że zawarty w nim wykaz nie ma ograniczającego charakteru, oznacza według mnie, że praktyki lub mechanizmy, które nie opierają się na dostępnej i przewidywalnej podstawie prawnej, mogą być uwzględniane w ramach całościowej oceny stopnia ochrony, jaki zapewnia to państwo trzecie, po to by uzupełnić te zabezpieczenia, które mają podstawę prawną wykazującą takie cechy. Jak jednak zauważyli zasadniczo DPC, M. Schrems, rząd austriacki i EROD, podobne praktyki lub mechanizmy nie mogą zastąpić tego rodzaju zabezpieczeń, i, co za tym idzie, samodzielnie zapewnić wymaganego stopnia ochrony.

3) Warunek dotyczący braku naruszenia istoty praw podstawowych

272. Zawarty w art. 52 ust. 1 karty wymóg, zgodnie z którym wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w karcie muszą respektować istotę tych praw i wolności, oznacza, że w przypadku, gdy ingerencja stanowi jej naruszenie, żaden uprawniony cel nie może być uzasadnieniem dla takiej ingerencji. Ingerencja jest wtedy uważana za niezgodną z kartą bez konieczności badania tego, czy jest ona odpowiednia i konieczna do realizacji celu, jakiemu służy ustanowione ograniczenie.

273. Trybunał orzekł w tym względzie, że uregulowanie krajowe pozwalające organom publicznym na uzyskanie generalnego dostępu do *treści* komunikatów elektronicznych narusza istotę prawa podstawowego do poszanowania życia prywatnego, wynikającego z art. 7 karty¹⁴⁷. Natomiast jeśli chodzi o dostęp do *danych o ruchu i lokalizacji*¹⁴⁸, Trybunał uznał (podkreślając jednocześnie ryzyka związane z dostępem do takich danych i ich analizowaniem), że istota tego prawa nie jest zagrożona, gdy przepis krajowy umożliwia organom państwowym generalny dostęp do tych danych¹⁴⁹.

274. Nie można moim zdaniem uznać, że art. 702 FISA upoważnia amerykańskie organy wywiadu do dostępu na zasadzie powszechności, do treści komunikatów elektronicznych.

275. Po pierwsze, dostęp organów wywiadu do danych na podstawie art. 702 FISA do celów związanych z ich *analizowaniem* i ewentualnym *wykorzystaniem* jest bowiem ograniczony do danych spełniających kryteria selekcji skojarzone z konkretnymi celami.

¹⁴⁶ Zobacz również motyw 104 RODO.

¹⁴⁷ Zobacz wyrok Schrems (pkt 94). Zobacz również wyroki Digital Rights Ireland (pkt 39) i Tele2 Sverige (pkt 101). Mając na względzie ścisły związek, jaki zachodzi pomiędzy prawem do poszanowania życia prywatnego a ochroną danych osobowych, przepis krajowy umożliwiający organom publicznym generalny dostęp do treści komunikatów naruszałby również, jak się wydaje, istotę prawa ustanowionego na mocy art. 8 karty.

¹⁴⁸ Zobacz pkt 257 niniejszej opinii. W wyroku Tele2 Sverige (pkt 99), Trybunał podkreślił, że te metadane umożliwiają w szczególności ustalenie profilu osób, których dane dotyczą. Grupa robocza z art. 29 w swojej opinii 04/2014 z dnia 10 kwietnia 2014 r. w sprawie nadzoru komunikacji elektronicznej na potrzeby wywiadu i bezpieczeństwa narodowego WP 215 (s. 5), zwróciła uwagę, że metadane komunikatów są, ze względu na ich ustrukturyzowany charakter, łatwiejsze do gromadzenia i analizowania niż treść tych komunikatów.

¹⁴⁹ Zobacz wyrok Tele2 Sverige (pkt 99). W związku z ewoluowaniem technologii i sposobów komunikowania się, niektórzy komentatorzy zastanawiają się nad zasadnością wprowadzania rozróżnienia pomiędzy uogólnionym dostępem do treści komunikatów a uogólnionym dostępem do metadanych, zob. N. Falot i H. Hijmans, Tele2: de afweging tussen privacy en veiligheid nader omlijnd, *Nederlands Tijdschrift voor Europees Recht*, nr 3, 2017 r. (s. 48) oraz T. Ojanen, Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter (glosa do wyroku Schrems), *European Constitutional Law Review*, 2016 (s. 5).

276. Po drugie, prawdą jest, że program Upstream mógłby wiązać się z uogólnionym dostępem do treści komunikatów elektronicznych *na potrzeby ich zautomatyzowanego filtrowania* w przypadkach, gdyby selektory stosowane nie tylko do pól „od” i „do”, lecz również do całej zawartości przepływu komunikatów (wyszukiwanie „na temat” selektora)¹⁵⁰. Jednakże, jak twierdzi Komisja, i wbrew temu, co zarzucają M. Schrems i EPIC, czasowy dostęp organów wywiadu do ogółu treści komunikatów elektronicznych wyłącznie na potrzeby ich filtrowania z zastosowaniem kryteriów selekcji nie może być utożsamiany z uogólnionym dostępem do tych treści¹⁵¹. Moim zdaniem waga ingerencji wynikających z tego ograniczonego w czasie dostępu w celu zautomatyzowanego filtrowania nie jest równa wadze ingerencji wynikających z generalnego udostępnienia tych treści organom publicznym na potrzeby ich analizowania i ewentualnego wykorzystania¹⁵². Czasowy dostęp na potrzeby filtrowania nie umożliwia tym organom zatrzymywania metadanych lub treści komunikatów, które nie spełniają kryteriów selekcji, ani, w szczególności (jak zauważył rząd amerykański), określania profili dotyczących osób, które nie zostały namierzone przy pomocy tych kryteriów.

277. Kwestia ustalenia, czy namierzanie przy użyciu selektorów w ramach programów opierających się na art. 702 FISA skutecznie ogranicza uprawnienia organów wywiadu, zależy jednak od uregulowania dotyczącego wyboru selektorów¹⁵³. Maximilian Schrems podnosi w tym względzie, że w związku z brakiem dostatecznej kontroli w tym zakresie prawo amerykańskie nie przewiduje zabezpieczeń przed uogólnionym dostępem do treści komunikatów już na etapie filtrowania, w związku z czym narusza ono samą istotę prawa do poszanowania życia prywatnego przysługującego osobom, których dane dotyczą.

278. Jak wyjaśnię bardziej szczegółowo w dalszej części opinii¹⁵⁴, jestem skłonny podzielić te wątpliwości co do wystarczającego charakteru regulacji dotyczących wyboru selektorów na potrzeby spełnienia kryteriów przewidywalności i proporcjonalności ingerencji. Jednakże istnienie tych regulacji, nawet jeśli są niedoskonałe, nie pozwala wnioskować, że art. 702 FISA upoważnia organy publiczne do uogólnionego dostępu do treści komunikatów elektronicznych, i w związku z tym stanowi naruszenie samej istoty prawa ustanowionego na mocy art. 7 karty.

279. Chciałbym również podkreślić, że Trybunał w opinii 1/15 uznał, że istota prawa do ochrony danych osobowych ustanowionego w art. 8 karty jest zachowana, jeżeli cele przetwarzania są ograniczone i jeżeli przetwarzaniu towarzyszą normy służące zapewnieniu w szczególności bezpieczeństwa, poufności i integralności tych danych, a także ochrony przed niezgodnymi z prawem wypadkami dostępu do nich i ich przetwarzania¹⁵⁵.

150 Zobacz przypis 87 do decyzji w sprawie Tarczy Prywatności. Jednakże, zgodnie z uwagami EPIC oraz z udzieloną na piśmie odpowiedzią rządu Stanów Zjednoczonych na pytania zadane przez Trybunał, w 2017 r. FISC zażądał zawieszenia wyszukiwań „na temat” selektora z uwagi na nieprawidłowości, jakimi było obarczone tego rodzaju wyszukiwanie. Jednakże Kongres, w przyjętej w 2018 r. ustawie ponownie zatwierdzającej FISA, przewidział możliwość ponownego wprowadzenia tego rodzaju wyszukiwania za zgodą FISC i Kongresu. Zobacz również EROD, EU-U.S. Privacy Shield – Second Annual Joint Review, 22 stycznia 2019 r. (s. 27, pkt 55).

151 W tym kontekście sąd odsyłający w pkt 188 i 189 wyroku z dnia 3 października 2017 r. wprowadza rozróżnienie pomiędzy „hurtowym” wyszukiwaniem a „hurtowym” pozyskiwaniem, zbieraniem lub zatrzymywaniem. Sąd ten uważa w istocie, że chociaż program Upstream wiąże się z „hurtowym” wyszukiwaniem odnoszącym się do ogółu danych, które przepływają przez telekomunikacyjną „infrastrukturę szkieletową”, to działania polegające na pozyskiwaniu, zbieraniu i zatrzymywaniu są ukierunkowane w ten sposób, że ich przedmiotem są wyłącznie dane zawierające rozpatrywane selektory.

152 Zobacz podobnie wyrok Supreme Court (sądu najwyższego) z dnia 31 maja 2019 r. (pkt 11.2 i 11.3). Sąd ten zwraca w nim uwagę, że: „[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term »processing« covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis”.

153 Zobacz opinię 1/15 (pkt 122). Zobacz również sprawozdanie Europejskiej Komisji na rzecz Demokracji przez Prawo (Komisji Weneckiej) z dnia 15 grudnia 2015 r. dotyczące demokratycznej kontroli nad agencjami wywiadu elektromagnetycznego, opracowanie nr 719/2013 [CDL-AD(2015)011, s. 11]: „W praktyce stwierdzenie, czy proces ten odpowiednio ogranicza nadmierne ingerencje w nieszkodliwe osobiste komunikaty, zależy od ustalenia, czy selektor jest dostatecznie trafny i konkretny oraz czy jakoś algorytmu programu używanego do identyfikowania odpowiednich danych w ramach wybranych parametrów jest dostateczna [...]”.

154 Zobacz pkt 297–301 niniejszej opinii.

155 Opinia 1/15 (pkt 150).

280. W decyzji w sprawie Tarczy Prywatności Komisja stwierdziła, że zarówno art. 702 FISA, jak też PPD 28 wprowadzają ograniczenia, jeśli chodzi o cele, do jakich dane mogą być zbierane w ramach programów wdrożonych na podstawie art. 702 FISA¹⁵⁶. W decyzji tej Komisja zwróciła również uwagę, że PPD 28 przewiduje zasady regulujące dostęp do danych oraz ich przechowywanie i rozpowszechnianie, tak aby zapewnić ich bezpieczeństwo i uchronić je przed nieuprawnionym dostępem¹⁵⁷. W dalszej części mojego wywodu wyjaśnię¹⁵⁸, że moje wątpliwości budzi w szczególności to, czy cele omawianego przetwarzania danych są zdefiniowane na tyle jasno i precyzyjnie, aby zapewnić stopień ochrony równoważny pod względem merytorycznym z tym, który obowiązuje w porządku prawnym Unii. Jednakże te ewentualne niedociągnięcia według mnie nie są wystarczające dla uzasadnienia twierdzenia, zgodnie z którym tego rodzaju programy, gdyby zostały wdrożone w Unii, naruszałyby istotę prawa do ochrony danych osobowych.

281. Poza tym przypominam, że adekwatność stopnia ochrony zapewnianą w związku z prowadzeniem nadzoru na podstawie EO 12333 należy oceniać w świetle postanowień EKPC. Z decyzji w sprawie Tarczy Prywatności wynika w tym względzie, że jedynymi ograniczeniami odnoszącymi się do wdrażania środków opartych na EO 12333 w celu zbierania danych o osobach niebędących obywatelami ani rezydentami amerykańskimi są ograniczenia przewidziane w PPD 28¹⁵⁹. Ta prezydencka dyrektywa stanowi, że wykorzystanie wywiadu powinno być „w najwyższym możliwym stopniu ukierunkowane”. Jednakże akt ten zawiera jednoznaczne stwierdzenie o możliwości „hurtowego” zbierania danych poza terytorium amerykańskim, w związku z realizacją pewnych szczególnych celów w obszarze bezpieczeństwa narodowego¹⁶⁰. Zdaniem M. Schremsa przepisy PPD 28, poza tym, że nie przyznają praw jednostkom, nie udzielają osobom, których dane dotyczą, ochrony przed ryzykiem powszechnego dostępu do ich komunikatów elektronicznych.

282. Jeśli chodzi o tę kwestię, ograniczę się do stwierdzenia, że ETPC w swoim orzecznictwie dotyczącym art. 8 EKPC, nie stosuje konceptu naruszenia istoty lub samej kwintesencji prawa do poszanowania życia prywatnego¹⁶¹. ETPC nie stwierdził do tej pory, że zasady umożliwiające przechwytywanie (nawet na skalę masową) komunikatów elektronicznych, *jako takie wykraczają poza zakres swobodnego uznania państw członkowskich*. ETPC stoi na stanowisku, że tego rodzaju zasady są zgodne z art. 8 ust. 2 EKPC, jeżeli towarzyszy im szereg minimalnych zabezpieczeń¹⁶². W tych

¹⁵⁶ Zobacz motywy 70, 103 i 109 decyzji w sprawie Tarczy Prywatności.

¹⁵⁷ Zobacz motywy 83–87 oraz załącznik VI, pkt I lit. c) decyzji w sprawie Tarczy Prywatności. Zwracam uwagę, że zgodnie ze sprawozdaniem PCLOB (s. 51–66), procedury „minimalizacji” stosowane przez NSA na podstawie art. 702 FISA w większości aspektów dotyczą wyłącznie obywateli amerykańskich. PPD 28 miała na celu rozszerzenie zakresu wynikających z tego aktu zabezpieczeń mających zastosowanie w przypadku osób niebędących obywatelami ani rezydentami amerykańskimi. Zobacz PCLOB, Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities, disponible à l'adresse <https://www.pclob.gov/reports/report-PPD28/> (s. 2). Jednakże przechowywanie i wykorzystywanie danych do celów bezpieczeństwa narodowego, po ich pozyskaniu przez organy publiczne, moim zdaniem nie jest objęte zakresem stosowania prawa Unii (zob. pkt 226 niniejszej opinii). Adekwatność stopnia ochrony zapewnianego w ramach tej działalności należy zatem oceniać wyłącznie w świetle art. 8 EKPC.

¹⁵⁸ Zobacz pkt 283–289 niniejszej opinii.

¹⁵⁹ W motywie 127 decyzji w sprawie Tarczy Prywatności Komisja stwierdziła między innymi, że czwarta poprawka do konstytucji Stanów Zjednoczonych nie ma zastosowania do osób niebędących obywatelami ani rezydentami amerykańskimi.

¹⁶⁰ Zobacz motywy 73 i 74 oraz załącznik VI pkt I lit. b) decyzji w sprawie Tarczy Prywatności. Cele te obejmują zwalczanie działalności szpiegowskiej i innych zagrożeń i rodzajów działalności skierowanych przez obce mocarstwa przeciwko Stanom Zjednoczonym i ich interesom; zwalczanie zagrożeń terrorystycznych; zagrożeń wynikających z rozwoju, posiadania, rozpowszechniania i stosowania broni masowego rażenia; zagrożeń dla bezpieczeństwa cybernetycznego; zagrożeń dla sił zbrojnych Stanów Zjednoczonych lub ich sojuszników oraz zagrożeń związanych z przestępczością międzynarodową. Zgodnie z brzmieniem przypisu na s. 5 PPD 28, ograniczenie celów uzasadniających wykorzystywanie danych zgromadzonych „hurtowo” nie ma zastosowania w sytuacji, gdy takie gromadzenie ma jedynie tymczasowy charakter i ma ułatwiać gromadzenie bardziej ukierunkowane.

¹⁶¹ Mimo że postanowienia EKPC nie zawierają odwołania do pojęcia „istoty” praw podstawowych, w orzecznictwie ETPC dotyczącym niektórych z tych postanowień pojawia się wyrażenie „kwintesencja” prawa podstawowego stanowiące odpowiednik tego pojęcia. Jeśli chodzi o kwintesencję prawa do rzetelnego procesu zagwarantowanego w art. 6 EKPC, zob. w szczególności wyroki ETPC z dnia 25 maja 1985 r., Ashingdane przeciwko Zjednoczonemu Królestwu (CE:ECHR:1985:0528JUD000822578, § 57 i 59); z dnia 21 grudnia 2000 r., Heaney and McGuinness przeciwko Irlandii (CE:ECHR:2000:1221JUD003472097, § 55 i 58); z dnia 23 czerwca 2016 r., Baka przeciwko Węgrom (CE:ECHR:2016:0623JUD002026112, § 121). Co się tyczy kwintesencji prawa do zawarcia małżeństwa ustanowionego w art. 12 EKPC, zob. wyrok ETPC z dnia 11 lipca 2002 r., Christine Goodwin przeciwko Zjednoczonemu Królestwu (CE:ECHR:2002:0711JUD002895795, § 99 i 101). Jeśli chodzi o kwintesencję prawa do nauki zagwarantowanego w art. 2 Protokołu nr 1 do EKPC, zob. wyrok ETPC z dnia 23 lipca 1968 r., sprawa „dotycząca niektórych aspektów językowych szkolnictwa w Belgii” (CE:ECHR:1968:0723JUD000147462, § 5).

¹⁶² Zobacz w szczególności wyroki Centrum för Rättvisa (§ 112–114 i przytoczone tam orzecznictwo) i Big Brother Watch (§ 337).

okolicznościach nie uważam, aby właściwe było formułowanie wniosków, iż zasady inwigilacji takie te ustanowione w EO 12333 wykraczałyby poza zakres swobodnego uznania państw członkowskich, *wyłącznie z tego powodu*, że umożliwiają one nieukierunkowane zbieranie treści komunikatów elektronicznych, bez przeprowadzenia jakiegokolwiek badania ewentualnych zabezpieczeń towarzyszących tym zasadom.

4) W przedmiocie warunku dotyczącego dążenia do prawnie uzasadnionego celu

283. Zgodnie z art. 52 ust. 1 karty wszelkie ograniczenia w korzystaniu z ustanowionych w niej praw powinny rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię. Artykuł 8 ust. 2 karty stanowi również, że przetwarzanie danych osobowych, które nie odbywa się na podstawie zgody osoby, której dane dotyczą, powinno odbywać się „na innej uzasadnionej podstawie przewidzianej ustawą”. W art. 8 ust. 2 EKPC wyliczono natomiast cele mogące uzasadniać ingerencję w korzystanie z prawa do poszanowania życia prywatnego.

284. Na mocy decyzji w sprawie Tarczy Prywatności zobowiązanie do przestrzegania wyrażonych w niej zasad może być ograniczone w celu wypełnienia obowiązków odnoszących się do bezpieczeństwa narodowego, interesu publicznego i przestrzegania prawa¹⁶³. W motywach 67–124 tej decyzji zawarta jest bardziej szczegółowa analiza ograniczeń spowodowanych uzyskiwaniem dostępu do danych przez amerykańskie organy publiczne i ich wykorzystaniem przez te organy do celów bezpieczeństwa narodowego.

285. Bezsporne jest, że ochrona bezpieczeństwa narodowego stanowi prawnie uzasadniony cel mogący uzasadniać odstępstwa od wymogów RODO¹⁶⁴, od korzystania z praw podstawowych ustanowionych w art. 7 i 8 karty¹⁶⁵, a nawet art. 8 ust. 2 EKPC. Jednakże M. Schrems, rząd austriacki i EPIC zwrócili uwagę, że cele realizowane w ramach programów nadzoru opartych na art. 702 FISA oraz na EO 12333 wykraczają poza samo bezpieczeństwo narodowe. Zgodnie z brzmieniem tych aktów prawnych, ich celem jest bowiem pozyskanie „zagranicznych informacji wywiadowczych”, które to pojęcie obejmuje różne rodzaje informacji, w tym te odnoszące się do bezpieczeństwa narodowego, lecz nie ogranicza się do nich¹⁶⁶. Zakresem pojęcia „zagranicznych informacji wywiadowczych” w rozumieniu art. 702 FISA objęte są bowiem dane dotyczące prowadzenia spraw zagranicznych¹⁶⁷. Z kolei EO 12333 definiuje to pojęcie w taki sposób, że obejmuje ono informacje odnoszące się do możliwości, zamiarów lub działalności obcych rządów, zagranicznych organizacji lub cudzoziemców¹⁶⁸. Maximilian Schrems kwestionuje zgodność z prawem określonego w ten sposób celu, ponieważ wykracza on poza bezpieczeństwo narodowe.

¹⁶³ Zobacz pkt 197 niniejszej opinii.

¹⁶⁴ Zobacz art. 23 ust. 1 lit. a) RODO.

¹⁶⁵ Zobacz wyrok Schrems (pkt 88). Trybunał uznał pokrewne pojęcie „bezpieczeństwa publicznego” w rozumieniu postanowień TFUE (zezwalających na odstępstwa od gwarantowanych w tym traktacie swobód podstawowych) za autonomiczne pojęcie prawa Unii obejmujące zarówno bezpieczeństwo wewnętrzne jak i zewnętrzne państw członkowskich [zob. między innymi wyroki z dnia 26 października 1999 r., Sirdar (C-273/97, EU:C:1999:523, pkt 17); z dnia 13 września 2016 r., CS (C-304/14, EU:C:2016:674, pkt 39 i przytoczone tam orzecznictwo)]. Podczas gdy bezpieczeństwo wewnętrzne może zostać zakłócone w szczególności poprzez bezpośrednie zagrożenie spokoju i fizycznego bezpieczeństwa ludności danego państwa członkowskiego, bezpieczeństwo zewnętrzne może zostać zagrożone, w szczególności, przez ryzyko poważnego zakłócenia stosunków zagranicznych tego państwa członkowskiego lub pokojowego współistnienia narodów. Mimo że państwa członkowskie nie mogą jednostronnie określać treści tych pojęć, to dysponują one jednak pewnym zakresem uznania na potrzeby definiowania swoich podstawowych interesów w zakresie bezpieczeństwa. Zobacz w szczególności wyrok z dnia 2 maja 2018 r., K. i H.F. (Zezwolenie na pobyt i zarzuty udziału w zbrodniach wojennych) (sprawy połączone C-331/16 i C-366/16, EU:C:2018:296, pkt 40–42 i przytoczone tam orzecznictwo). Moim zdaniem, rozważania te można przenieść na grunt wykładni pojęcia „bezpieczeństwa narodowego” jako interesu, którego ochrona może uzasadniać ograniczenia stosowania przepisów RODO i praw gwarantowanych w art. 7 i 8 karty.

¹⁶⁶ Zobacz w tym względzie motyw 89 i przypis 97 do decyzji w sprawie Tarczy Prywatności.

¹⁶⁷ Zobacz pkt 55 niniejszej opinii.

¹⁶⁸ Zobacz pkt 61 niniejszej opinii.

286. Moim zdaniem zakres pojęcia bezpieczeństwa narodowego może obejmować w pewnej mierze, ochronę interesów związanych z prowadzeniem spraw zagranicznych¹⁶⁹. Poza tym nie można wykluczyć, że pewne inne niż ochrona bezpieczeństwa narodowego cele wchodzące w zakres pojęcia „zagranicznych informacji wywiadowczych” zdefiniowanego w art. 702 FISA i w EO 12333, odpowiadają prawnie uzasadnionym ważnym celom leżącym w interesie ogólnym i mogącym uzasadniać ingerencję w prawa podstawowe, jakimi są prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych. Te cele mają jednak, w kontekście wyważania praw podstawowych osób, których dane dotyczą, i celu, jakiemu służy ingerencja, mniejszą wagę niż ochrona bezpieczeństwa narodowego¹⁷⁰.

287. Jednakże zgodnie z art. 52 ust. 1 karty, konieczne jest jeszcze, aby akty prawne, które przewidują takie ingerencje, rzeczywiście służyły bezpieczeństwu narodowemu albo innemu prawnie uzasadnionemu celowi¹⁷¹. Poza tym, cele ingerencji powinny być określone w sposób odpowiadający wymogom jasności i precyzji¹⁷².

288. Tymczasem zdaniem M. Schremsa, cel zawarty w art. 702 FISA oraz w EO 12333 środków umożliwiających inwigilację, nie jest sformułowany ma tyle precyzyjnie, aby spełnić wymogi przewidywalności i proporcjonalności. Jest tak między innymi dlatego, że środki te zawierają niezwykle szeroką definicję pojęcia „zagranicznych informacji wywiadowczych”. Ponadto Komisja stwierdziła w motywie 109 decyzji w sprawie Tarczy Prywatności, że art. 702 FISA wymaga, aby „istotnym celem” gromadzenia informacji było pozyskanie zagranicznych informacji wywiadowczych, które to sformułowanie, jak zauważyło EPIC, na pierwszy rzut oka nie wyklucza realizacji innych, nieokreślonych celów.

289. Z powyższych względów, nie wykluczając, że przewidziane w art. 702 FISA lub w EO 12333 środki nadzorcze służą realizacji prawnie uzasadnionych celów, można się zastanawiać, czy cele te są zdefiniowane w sposób na tyle jasny i precyzyjny, aby zapobiec ryzyku nadużyć i umożliwić kontrolę proporcjonalności ingerencji, jakie niosą ze sobą te środki¹⁷³.

5) W przedmiocie niezbędności i proporcjonalności ingerencji

290. Trybunał wielokrotnie podkreślał, że prawa ustanowione w art. 7 i 8 karty nie są prawami bezwzględnymi, ale że należy ich postrzegać w kontekście ich funkcji społecznej i dokonywać ich wyważenia względem innych praw podstawowych, w myśl zasady proporcjonalności¹⁷⁴. Jak podkreśliła Facebook Ireland, wśród tych praw znajduje się prawo do bezpieczeństwa osobistego gwarantowane w art. 6 karty.

169 W wyroku Centrum för Rättvisa (§ 111) ETPC orzekł, że prowadzenie inwigilacji w celu wspierania szwedzkiej polityki zagranicznej, polityki obronnej i polityki bezpieczeństwa oraz w celu wykrywania organizowanych w Szwecji zagrożeń pochodzących z zewnątrz, służy prawnie uzasadnionym celom związanym z bezpieczeństwem narodowym.

170 Zobacz na ten temat wyrok Tele2 Sverige (pkt 115) i wyrok Ministerio Fiscal (pkt 55). W wyrokach tych Trybunał podkreślił związek pomiędzy wagą ingerencji a wagą interesu, który jest powoływany jako jej uzasadnienie.

171 Grupa robocza z art. 29 w swoim dokumencie roboczym z dnia 5 grudnia 2014 r., dotyczącym inwigilacji komunikacji elektronicznej na potrzeby wywiadu i bezpieczeństwa narodowego, WP 228 (s. 27), podkreśliła znaczenie, jakie ma dokonanie krytycznej oceny tego, czy nadzór ten jest rzeczywiście sprawowany do celów bezpieczeństwa narodowego.

172 Zobacz opinię 1/15 (pkt 181), w której Trybunał orzekł, że treść przepisów ustawowych przewidujących ingerencje nie spełnia wymogów jasności i precyzji, co powoduje, że takie ingerencje nie są ograniczone do tego, co ściśle konieczne. Zgodnie z tym samym podejściem, rzecznik generalny Y. Bot w swojej opinii w sprawie Schrems (C-362/14, EU:C:2015:627, pkt 181–184) uznał, że cele aktów prawnych przewidujących sprawowanie nadzoru (były sformułowane za mało precyzyjnie, aby można było uznać je za cele leżące w interesie ogólnym (z wyłączeniem bezpieczeństwa narodowego)).

173 Podobne wątpliwości zostały wyrażone przez Europejskiego Inspektora Ochrony Danych w jego opinii 4/2016 z dnia 30 maja 2016 r. dotyczącej Tarczy Prywatności UE–Stany Zjednoczone (Privacy Shield) – Projekt decyzji stwierdzającej odpowiedni stopień ochrony (s. 8).

174 Zobacz wyrok z dnia 9 listopada 2010 r., Volker und Markus Schecke i Eifert (sprawy połączone C-92/09 i C-93/09, EU:C:2010:662, pkt 48); opinia 1/15 (pkt 136); wyrok z dnia 24 września 2019 r., Google (Zakres terytorialny prawa do usunięcia linków) (C-507/17, EU:C:2019:772, pkt 60).

291. W tym względzie, zgodnie z równie utrwalonym orzecnictwem, jakkolwiek ingerencja w korzystanie z praw zagwarantowanych w art. 7 i 8 karty powinna podlegać ścisłej kontroli pod względem proporcjonalności¹⁷⁵.

292. Z wyroku Schrems wynika w szczególności, że „uregulowanie umożliwiające generalnie przechowywanie wszelkich danych osobowych [...] bez jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od zamierzonego celu i bez przewidzenia obiektywnych kryteriów, które pozwoliłyby na ograniczenie dostępu władz publicznych do danych oraz na ich późniejsze wykorzystanie do określonych celów, ściśle ograniczonych, które mogą uzasadnić ingerencję, jaką stanowi zarówno dostęp, jak i wykorzystanie tych danych, nie ogranicza się do tego, co absolutnie konieczne.”¹⁷⁶.

293. Trybunał orzekł również, że, z wyjątkiem należycie uzasadnionych pilnych przypadków, dostęp do danych powinien być uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, którego orzeczenia służą ograniczaniu dostępu do danych oraz ich wykorzystania, do sytuacji ściśle koniecznych dla osiągnięcia zamierzonego celu¹⁷⁷.

294. Obecnie art. 23 ust. 2 RODO ustanawia szereg zabezpieczeń, jakie powinno ustanowić państwo członkowskie, gdy wprowadza odstępstwa od przepisów tego rozporządzenia. Akt prawny zezwalający na zastosowanie takiego odstępstwa powinien zawierać przepisy odnoszące się między innymi do celów przetwarzania, zakresu wprowadzanego odstępstwa, zabezpieczeń zapobiegających nadużyciom, okresów przechowywania oraz prawa osób, których dane dotyczą, do uzyskania informacji o odstępstwie, o ile nie narusza to celu tego odstępstwa.

295. W niniejszej sprawie M. Schrems twierdzi, że regulacji zawartej w art. 702 FISA nie towarzyszą zabezpieczenia dostateczne do tego, aby zapobiec występowaniu nadużyć i uzyskiwaniu nieuprawnionego dostępu do danych. W szczególności wybór kryteriów selekcji nie jest dostatecznie uregulowany, co sprawia, że przepis ten nie zabezpiecza przed uogólnionym dostępem do treści komunikatów.

296. Rząd Stanów Zjednoczonych i Komisja twierdzą natomiast, że art. 702 FISA ogranicza wybór selektorów przy pomocy obiektywnych kryteriów, ponieważ przepis ten umożliwia wyłącznie gromadzenie zawartych w komunikatach elektronicznych danych pochodzących od osób niebędących obywatelami czy też rezydentami amerykańskimi w celu pozyskania zagranicznych informacji wywiadowczych.

297. Moim zdaniem wątpliwe jest, czy te kryteria regulujące wybór selektorów są dostatecznie jasne i precyzyjne oraz czy istnieją zabezpieczenia wystarczające do tego, aby zapobiegać wystąpieniu nadużyć.

298. Przede wszystkim, w motywie 109 decyzji w sprawie Tarczy Prywatności przewidziano, że selektory, przed ich zastosowaniem, nie są indywidualnie zatwierdzane przez FISC ani przez inny niezależny organ sądowy lub administracyjny. W decyzji tej Komisja stwierdziła, że „[FISC] nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; może jednak zatwierdzać programy nadzoru [...] w oparciu o roczne certyfikacje”, co zostało potwierdzone przez rząd Stanów Zjednoczonych przed Trybunałem. W motywie tym wskazano, że „certyfikacje, które mają zostać zatwierdzone przez [FISC], nie zawierają żadnych informacji na temat poszczególnych osób, które mają być namierzane – [lecz raczej] służą one identyfikowaniu kategorii zagranicznych informacji

175 Zobacz między innymi wyrok z dnia 16 grudnia 2008 r., Satakunnan Markkinapörssi i Satamedia (C-73/07, EU:C:2008:727, pkt 56); wyrok Digital Rights Ireland (pkt 48 i 52); wyrok Schrems (pkt 78 i 92); opinia 1/15 (pkt 139 i 140). Zobacz również motyw 140 decyzji w sprawie Tarczy Prywatności.

176 Wyrok Schrems (pkt 93). Zobacz również podobnie wyrok Digital Rights Ireland (pkt 60).

177 Zobacz wyrok Tele2 Sverige (pkt 120) i opinię 1/15 (pkt 202).

wywiadowczych”, które mogą być zbierane. W tym samym motywie Komisja stwierdza również, że „[FISC] nie ocenia – na podstawie uzasadnionego podejrzenia lub innej normy – czy osoby fizyczne są odpowiednio namierzane do celów pozyskiwania zagranicznych informacji wywiadowczych”, mimo że kontroluje on spełnienie warunku, zgodnie z którym „istotnym celem gromadzenia informacji jest pozyskanie zagranicznych informacji wywiadowczych”.

299. Następnie, zgodnie z powyższym motywem, art. 702 FISA upoważnia NSA do gromadzenia komunikatów wyłącznie w sytuacji, gdy „istnieje uzasadnione podejrzenie, że [...] określon[y] środek] komunikacji [jest wykorzystywany] w celu przekazywania zagranicznych informacji wywiadowczych”. W motywie 70 decyzji w sprawie Tarczy Prywatności dodano, że wybór selektorów odbywa się w ogólnych ramach amerykańskich priorytetów wywiadowczych (National Intelligence Priorities Framework, NIPF). W decyzji tej nie stwierdzono, że istnieją wymogi bardziej szczegółowego uzasadnienia lub usprawiedliwienia wyboru selektorów w świetle tych obowiązujących NSA priorytetów administracyjnych¹⁷⁸.

300. Wreszcie, w motywie 71 decyzji w sprawie Tarczy Prywatności wskazano na przewidziany w PPD 28 wymóg, zgodnie z którym proces gromadzenia zagranicznych informacji wywiadowczych musi być „w jak największym stopniu dostosowany do indywidualnych potrzeb”. Niezależnie od okoliczności, że ta dyrektywa prezydencka nie przyznaje praw jednostkom, merytoryczna równowaga kryterium działalności „w jak największym stopniu dostosowanej do indywidualnych potrzeb” i kryterium „ściślej konieczności” ustanowionego w art. 52 ust. 1 karty dla uzasadnienia ingerencji w korzystanie z praw gwarantowanych w jej art. 7 i 8, nie wydaje mi się wcale oczywista¹⁷⁹.

301. Z powyższych względów, w świetle okoliczności przedstawionych w decyzji w sprawie Tarczy Prywatności, nie jest pewne, czy opartym na art. 702 FISA środkiem nadzorczym towarzyszą zabezpieczenia dotyczące ograniczenia kręgu osób, wobec których te środki mogą być stosowane, oraz celów, do jakich dane te mogą być gromadzone, a które to zabezpieczenia byłyby równoważne pod względem merytorycznym z zabezpieczeniami wymaganymi przez RODO w związku z art. 7 i 8 karty¹⁸⁰.

302. Poza tym, co się tyczy oceny adekwatności stopnia ochrony towarzyszącego nadzorowi sprawowanemu na podstawie EO 12333, to wprowadzie ETPC przyznaje państwom członkowskim szeroki zakres uznania, jeśli chodzi o wybór środków służących ochronie ich bezpieczeństwa narodowego, to jednak zakres ten jest ograniczony przez wymóg ustanowienia odpowiednich i wystarczających zabezpieczeń przed nadużyciami¹⁸¹. W swoim orzecznictwie dotyczącym środków nadzorczych ETPC bada, czy prawo wewnętrzne, będące podstawą stosowania tych środków, przewiduje skuteczne zabezpieczenia i gwarancje wystarczające dla spełnienia wymogów „przewidywalności” i „niezbędności w społeczeństwie demokratycznym”¹⁸².

178 W sprawozdaniu PCLOB (s. 45) wyjaśniono: „With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to »identify« the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification”.

179 Zobacz, podobnie, grupa robocza z art. 29, Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision, z dnia 13 kwietnia 2016 r., WP 238 (pkt 3.3.1, s. 38); Rezolucja Parlamentu Europejskiego z dnia 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez tzw. Tarczę Prywatności UE–USA (2016/3018(RSP)), P8_TA(2017)0131 (pkt 17); sprawozdanie Parlamentu Europejskiego z dnia 20 lutego 2017 r. w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw, A8–0044/2017 (pkt 17).

180 Zobacz, podobnie, grupa robocza z art. 29, EU-U.S. Privacy Shield – First Annual Joint Review, 28 listopada 2017 r., WP 255 (s. 3); Rezolucja Parlamentu Europejskiego z dnia 5 lipca 2018 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, P8_TA-PROV(2018)0315 (pkt 22); EROD, EU-U.S. Privacy Shield – Second Annual Joint Review, 22 stycznia 2019 r. (pkt 81–83 i 87).

181 Zobacz między innymi wyroki Zakharov (§ 232) oraz Szabó i Vissy (§ 57).

182 Zobacz między innymi wyroki Zakharov (§ 237); Centrüm för Rättvisa (§ 111); Big Brother Watch (§ 322).

303. ETPC wymienia w tym kontekście szereg minimalnych zabezpieczeń. Zabezpieczenia te dotyczą jasnego wskazania charakteru czynów zabronionych, których popełnienie może spowodować wydanie nakazu przechwytywania danych, definicji kategorii osób, których komunikaty mogą być przechwytywane, określenia maksymalnej długości okresu, w którym środek może być stosowany, procedury, jaką należy stosować na potrzeby analizowania, wykorzystania i przechowywania zgromadzonych danych, środków ostrożności, jakie należy podejmować w przypadku przekazywania danych innym podmiotom oraz okoliczności, w jakich zarejestrowane dane mogą lub muszą zostać usunięte¹⁸³.

304. Adekwatność i skuteczność zabezpieczeń towarzyszących ingerencjom zależy od całokształtu okoliczności danego przypadku, w tym od charakteru, zakresu i czasu trwania środków, przyczyn uzasadniających ich zastosowanie, organów właściwych do zezwalania na ich stosowanie, do ich stosowania oraz do kontroli nad nimi, jak również od rodzaju środków ochrony prawnej przysługujących na mocy prawa wewnętrznego¹⁸⁴.

305. Oceniając zasadność środka nadzorczego ETPC bierze w szczególności pod uwagę całokształt sprawowanej kontroli „w momencie wydania nakazu zastosowania środka”, „w czasie jego stosowania” oraz „po zakończeniu jego stosowania”¹⁸⁵. Co się tyczy pierwszego z tych trzech etapów, ETPC wymaga, aby zezwolenie na zastosowanie takiego środka wydawał niezawisły organ. Mimo że zdaniem ETPC władza sądownicza daje najlepsze gwarancje niezawisłości, bezstronności i prawidłowości postępowania, organ wydający takie zezwolenie nie musi konieczniej być organem sądowym¹⁸⁶. Pogłębiona kontrola sądowa na późniejszym etapie może zrównoważyć ewentualne uchybienia procedury wydawania zgody¹⁸⁷.

306. W niniejszej sprawie z decyzji w sprawie Tarczy Prywatności wynika, że jedyne zabezpieczenia, które ograniczają gromadzenie i wykorzystanie danych poza terytorium Stanów Zjednoczonych, zawarte zostały w PPD 28, ponieważ art. 702 FISA nie ma zastosowania poza tym terytorium. Nie jestem przekonany, czy zabezpieczenia te mogą wystarczyć do spełnienia warunków „przewidywalności” i „niezbędności w społeczeństwie demokratycznym”.

307. Przede wszystkim, jak już zauważyłem, ta dyrektywa prezydencka nie przyznaje praw jednostkom. Poza tym wątpię, że wymóg zapewnienia, aby nadzór był „w jak największym stopniu dostosowany do indywidualnych potrzeb” jest sformułowany w sposób na tyle jasny i precyzyjny, aby odpowiednio zabezpieczać osoby, których dane dotyczą, przed ryzykiem nadużyć¹⁸⁸. Wreszcie, w decyzji w sprawie Tarczy Prywatności nie zostało wykazane, że prowadzenie nadzoru w oparciu o EO 12333 jest poddawane uprzedniej kontroli sprawowanej przez niezawisły organ lub mogłoby być a posteriori przedmiotem kontroli sądowej¹⁸⁹.

308. W tych okolicznościach zasadność stwierdzenia, że Stany Zjednoczone, w ramach działalności prowadzonej przez ich służby wywiadowcze na podstawie sekcji 702 FISA oraz EO 12333, zapewniają odpowiedni stopień ochrony w rozumieniu art. 45 ust. 1 RODO w związku z art. 7 i 8 karty oraz art. 8 EKPC, budzi moje wątpliwości.

183 Zobacz między innymi rozstrzygnięcie Weber i Saravia (§ 95); wyrok ETPC z dnia 28 czerwca 2007 r., Association pour l'intégration européenne et les droits de l'homme et Ekimdjiev (CE:ECHR:2007:0628JUD006254000, § 76); a także wyrok Zakharov (§ 231).

184 Zobacz między innymi rozstrzygnięcie Weber i Saravia (§ 106); wyrok Zakharov (§ 232); wyrok Centrüm för Rättvisa (§ 104).

185 Zobacz między innymi wyrok ETPC z dnia 6 września 1978 r., Klass i in. przeciwko Niemcom (CE:ECHR:1978:0906JUD000502971, § 55); wyrok Zakharov (§ 233); wyrok Centrüm för Rättvisa (§ 105).

186 Zobacz między innymi wyrok Klass (§ 56); wyrok ETPC z dnia 18 maja 2010 r., Kennedy przeciwko Zjednoczonemu Królestwu (CE:ECHR:2010:0518JUD002683905, § 167); wyrok Zakharov (§ 233 i 258).

187 Zobacz wyroki Szabó i Vissy (§ 77) oraz Centrüm för Rättvisa (§ 133).

188 Wątpię w to tym bardziej z uwagi na okoliczności przedstawione w pkt 281 niniejszej opinii.

189 Zobacz pkt 330 i 331 niniejszej opinii.

c) Ważność decyzji w sprawie Tarczy Prywatności w świetle prawa do skutecznego środka prawnego

309. Piąte pytanie prejudycjalne wymaga od Trybunału ustalenia, czy osoby, których dane są przesyłane do Stanów Zjednoczonych, korzystają w tym państwie z ochrony sądowej, która jest równoważna pod względem merytorycznym z ochroną, jaka powinna być zapewniana w Unii na mocy art. 47 karty. W pytaniu dziesiątym sąd odsyłający pyta w istocie Trybunał, czy na pytanie piąte należy udzielić odpowiedzi twierdzącej z uwagi na mechanizm mediacji wprowadzony na podstawie decyzji w sprawie Tarczy Prywatności.

310. Na wstępie należy stwierdzić, że Komisja w motywie 115 tej decyzji uznała, iż w amerykańskim systemie prawnym istnieją luki, jeśli chodzi o ochronę sądową jednostek.

311. Zgodnie z tym motywem, po pierwsze, w przypadku „przynajmniej niektórych podstaw prawnych, na jakie mogą powołać się amerykańskie organy wywiadowcze (np. rozporządzenie wykonawcze nr 12333)” brak jest możliwości skorzystania ze środka ochrony prawnej przed sądem. Z treści EO 12333 i PPD 28 wynika bowiem, że te akty prawne nie przyznają praw osobom, których dane dotyczą, i nie mogą być przez te osoby powoływane przed sądami. Tymczasem skuteczna ochrona sądowa wymaga co najmniej, aby jednostki dysponowały prawami, na które mogą powołać się przed wymiarem sprawiedliwości.

312. Po drugie, „nawet jeżeli osoby niebędące obywatelami ani rezydentami USA mogą zasadniczo korzystać z sądowych środków odwoławczych, np. w przypadku nadzoru na mocy [FISA], dostępne podstawy wszczęcia powództwa są jednak ograniczone, a [zgłaszane roszczenia] [...] zostaną uznane za niedopuszczalne, jeżeli osoby te nie mogą wykazać interesu prawnego, co ogranicza dostęp do sądów powszechnych”.

313. Z motywów 116–124 decyzji w sprawie Tarczy Prywatności Komisja wynika, że instytucja rzecznika została ustanowiona na celu zrekompensowania tych ograniczeń. Komisja w motywie 139 tej decyzji stwierdziła, że „*mechanizmy nadzoru i mechanizmy odwoławcze przewidziane w Tarczy Prywatności – rozumiane jako całość – [...] oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do danych na ich temat oraz – ostatecznie – skorygowania lub usunięcia takich danych*” (wyróżnienie moje).

314. Przypominając ogólne zasady wynikające z orzecznictwa Trybunału i ETPC odnoszące się do prawa do wnoszenia środków odwoławczych przeciwko aktom prawnym dotyczącym inwigilacji komunikatów, przeanalizuję, czy przewidziane w prawie amerykańskim środki ochrony sądowej, takie jak te opisane w decyzji w sprawie Tarczy Prywatności, umożliwiają zapewnienie odpowiedniej ochrony sądowej osób, których dane dotyczą [część 1)]. Następnie ustalę, czy wprowadzenie pozasądowego mechanizmu mediacji pozwala w razie potrzeby, na wypełnienie ewentualnych luk w ochronie sądowej tych osób [część 2)].

1) W przedmiocie skuteczności przewidzianych w prawie Stanów Zjednoczonych środków ochrony prawnej

315. Przede wszystkim art. 47 akapit pierwszy karty stanowi, że każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem¹⁹⁰. Zgodnie z akapitem drugim tego postanowienia każdy ma prawo do rozpatrzenia jego sprawy przez niezawisły i bezstronny sąd¹⁹¹. Trybunał orzekł, że dostęp do niezawisłego sądu stanowi istotną treść prawa gwarantowanego przez art. 47 karty¹⁹².

316. Z tym prawem do indywidualnej ochrony sądowej łączy się spoczywający na państwach członkowskich i wynikający z art. 7 i 8 karty obowiązek poddania wszelkich środków mających na celu inwigilację (z wyłączeniem pilnych, należycie uzasadnionych przypadków) uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracji¹⁹³.

317. Co prawda, jak podnoszą rządy niemiecki i francuski, prawo do skutecznego środka ochrony prawnej przed sądem nie jest prawem bezwzględny¹⁹⁴, ponieważ może ono podlegać ograniczeniom ze względu na bezpieczeństwo narodowe. Jednakże odstępstwa są uzasadnione wyłącznie w zakresie, w jakim nie zagrażają istocie tego prawa i są niezbędne dla realizacji prawnie uzasadnionego celu.

318. Trybunał w wyroku Schrems orzekł w tym względzie, że uregulowanie nieprzewidujące dla jednostek *żadnej* drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty¹⁹⁵.

319. Należy podkreślić, że powyższe prawo dostępu wiąże się z tym, że dana osoba winna mieć możliwość uzyskania od organów publicznych (z zastrzeżeniem wyjątków absolutnie niezbędnych do realizacji prawnie uzasadnionego interesu) *potwierdzenia okoliczności, czy organy te przetwarzają dotyczące jej dane osobowe*¹⁹⁶. Takie jest moim zdaniem praktyczne znaczenie prawa dostępu w sytuacji, gdy zainteresowana osoba nie wie, czy organy publiczne zatrzymały jej dane osobowe, w szczególności po przeprowadzeniu zautomatyzowanego procesu filtrowania przepływu komunikatów elektronicznych.

190 W wyjaśnieniach dotyczących karty wskazano w tym względzie, że „w prawie Unii ochrona [ustanowiona w art. 47 karty] jest bardziej rozległa [niż ochrona przewidziana w art. 13 EKPC], ponieważ gwarantuje prawo do skutecznego środka prawnego przed sądem”. Zobacz również opinię rzecznika generalnego M. Watheleta w sprawie *Berlioz Investment Fund* (C-682/15, EU:C:2017:2, pkt 37).

191 Oceniając, w ramach stosowania art. 47 karty, czy dany organ posiada status „sądu”, należy uwzględnić ustawowe umocowanie organu, jego stały charakter, obligatoryjny charakter jego jurysdykcji, kontradyktoryjność postępowania, stosowanie przez ten organ przepisów prawa oraz jego niezawisłość. Zobacz wyrok z dnia 27 lutego 2018 r., *Associação Sindical dos Juízes Portugueses* (C-64/16, EU:C:2018:117, pkt 38 i przytoczone tam orzecznictwo).

192 Zobacz w szczególności wyroki z dnia 25 lipca 2018 r., *Minister for Justice and Equality (Nieprawidłowości w systemie sądownictwa)* (C-216/18 PPU, EU:C:2018:586, pkt 59 i 63), z dnia 5 listopada 2019 r., *Komisja/Polska ((Niezależność sądów powszechnych))* (C-192/18, EU:C:2019:924, pkt 106), i z dnia 19 listopada 2019 r., *A.K. i in. (Niezależność Izby Dyscyplinarnej Sądu Najwyższego)* (sprawy połączone C-585/18, C-624/18 i C-625/18, EU:C:2019:982, pkt 120).

193 Zobacz pkt 293 niniejszej opinii. Artykuł 45 ust. 3 lit a) RODO stanowi, że, oceniając, czy zapewniany przez państwo trzeci stopień ochrony jest odpowiedni, należy uwzględnić „administracyjne i sądowe środki zaskarżenia”, które mogą w tym państwie w sposób skuteczny wnosić osoby, których dane dotyczą (wyróżnienie moje). Podobnie, zgodnie z motywem 104 RODO, przyjęcie decyzji stwierdzającej odpowiedni stopień ochrony powinno być uwarunkowane tym, aby osoby, których dane dotyczą, uzyskały w danym państwie trzecim „skuteczne administracyjne i sądowe środki zaskarżenia” (wyróżnienie moje). Zobacz również, grupa robocza z art. 29, EU-U.S. Privacy Shield – First Annual Joint Review, 28 listopada 2017 r., WP 255 (pkt B.3); rezolucja Parlamentu Europejskiego z dnia 5 lipca 2018 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, P8_TA-PROV(2018)0315 (pkt 25 i 30); EROD, EU-U.S. Privacy Shield – Second Annual Joint Review, 22 stycznia 2019 r. (pkt 94–97).

194 Zobacz podobnie wyrok z dnia 28 lutego 2013 r., *Szczególna procedura kontroli orzeczenia Arango Jaramillo i in./EBI* (C-334/12 RX-II, EU:C:2013:134, pkt 43).

195 Wyrok Schrems (pkt 95).

196 Artykuł 15 RODO zatytułowany „Prawo dostępu przysługujące osobie, której dane dotyczą”, w ust. 1 stanowi, że osoba ta „jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich [...]”. Taką samą wymowę ma „zasada dostępu” przewidziana w załączniku II pkt II.8 lit. a) decyzji w sprawie Tarczy Prywatności.

320. Ponadto z orzecznictwa wynika, że organy państwa członkowskiego są co do zasady obowiązane poinformować o uzyskaniu dostępu do danych począwszy od chwili, w której informacja taka nie będzie mogła narazić na szwank prowadzonych przez te organy postępowań dochodzeniowo-śledczych¹⁹⁷. Taka informacja stanowi bowiem warunek wstępny skorzystania ze środka prawnego na podstawie art. 47 karty¹⁹⁸. Obowiązek ten wynika obecnie z art. 23 ust. 2 lit. h) RODO.

321. W motywach 111–135 decyzji w sprawie Tarczy Prywatności przedstawione zostały pokrótce wszystkie środki ochrony prawnej przysługujące osobom, których dane są przekazywane, gdy osoby te mają obawy, że te dane, po ich przekazaniu, były przetwarzane przez amerykańskie służby wywiadowcze. Te środki ochrony prawnej zostały również opisane w wyroku High Court (sądu najwyższego) z dnia 3 października 2017 r. załączonym do orzeczenia odsyłającego oraz w uwagach przedłożonych między innymi przez rząd Stanów Zjednoczonych.

322. Nie ma potrzeby szczegółowego przypominania treści tych wyjaśnień. Sąd odsyłający kwestionuje bowiem adekwatność zabezpieczeń odnoszących się do ochrony prawnej osób, których dane dotyczą, głównie z tego powodu, że szczególnie surowe wymogi dotyczące legitymacji procesowej (*standing*)¹⁹⁹ w połączeniu z brakiem obowiązku informowania osób, wobec których zastosowano nadzór *nawet wówczas, gdy udzielenie informacji nie zagrażałoby już celom*, w których ten nadzór jest prowadzony, powoduje w praktyce, że korzystanie ze środków ochrony prawnej przewidzianych w prawie Stanów Zjednoczonych jest nadmiernie utrudnione, a nawet – niemożliwe. DPC, M. Schrems, rządy austriacki, polski i portugalski oraz EROD dzielą tę wątpliwość²⁰⁰.

323. Jeśli chodzi o tę kwestię, ograniczę się tylko do przypomnienia, że zasady dotyczące legitymacji procesowej nie mogą naruszać prawa do skutecznej ochrony sądowej²⁰¹, oraz do stwierdzenia, że decyzją w sprawie Tarczy Prywatności nie przewiduje jakiegokolwiek wymogu informowania osób, których dane dotyczą, o tym, że stosowano wobec nich inwigilację²⁰². Skoro brak obowiązku informowania o inwigilacji (nawet gdy udzielenie informacji osobie, której dane dotyczą, nie zagrażałoby już jej skuteczności), mógłby przeszkodzić w korzystaniu z sądowych środków ochrony prawnej, brak ten wydaje się problematyczny w świetle orzecznictwa przytoczonego w pkt 320 niniejszej opinii.

197 Wyrok Tele2 Sverige (pkt 121); opinia 1/15 (pkt 220). Jak zauważyła spółka Facebook Ireland, nie można zatem w sposób systematyczny wymagać informowania o dostępie organów publicznych do danych. ETPC uważa w tym względzie, że „wymaganie udzielenia informacji a posteriori w praktyce może nie być możliwe”, ponieważ zagrożenie, w związku z którym wprowadzono środki nadzorcze, „może utrzymywać się przez lata, a nawet dziesięciolecia” po uchyleniu tych środków, tak że udzielenie informacji może „zagrozić długoterminowemu celowi, który pierwotnie uzasadniał nadzór” oraz „ujawnić metody pracy służb wywiadu, ich obszar działalności i [...] tożsamość ich agentów” [wyrok Zakharov (§ 287 i przytoczone tam orzecznictwo)]. W braku udzielenia takiej informacji, pomimo tego, że w przypadku naruszenia wymogów prawnych nie ma praktycznej możliwości skorzystania z indywidualnych środków ochrony prawnej, inne zabezpieczenia mogą być wystarczające do tego, aby chronić prawo do poszanowania życia prywatnego (zob. również wyrok Centrum för Rättvisa, § 164–167 i 171–178). Zobacz pkt 330 niniejszej opinii.

198 Zobacz w tym względzie przypis 210 do niniejszej opinii.

199 Zobacz pkt 67 niniejszej opinii.

200 Zobacz EROD, EU-U.S. Privacy Shield – Second Annual Joint Review, 22 stycznia 2019 r. (s. 18, pkt 97).

201 Zobacz między innymi wyroki z dnia 11 lipca 1991 r., Verholen i in. (sprawy połączone od C-87/90 do C-89/90, EU:C:1991:314, pkt 24 i przytoczone tam orzecznictwo); z dnia 28 lutego 2013 r., Szczególna procedura kontroli orzeczenia, Arango Jaramillo i in./BEI (C-334/12 RX-II, EU:C:2013:134, pkt 43).

202 Rząd Stanów Zjednoczonych wyjaśnił jednak, podobnie jak sąd odsyłający, że namierzana osoba powinna zostać poinformowana o środku nadzorczym zastosowanym na podstawie art. 702 FISA, jeżeli zgromadzone dane są wykorzystywane przeciwko niej w ramach postępowania sądowego.

324. Ponadto w przypisie 169 do decyzji w sprawie Tarczy Prywatności przyznano, że, aby móc skorzystać z dostępnych podstaw wszczęcia powództwa, „musi wystąpić szkoda [...] lub należy wykazać, że rząd zamierza wykorzystać lub ujawnić informacje uzyskane lub pochodzące z dozoru elektronicznego danej osoby przeciwko tej osobie [...]”. Jak zaznaczyli sąd odsyłający oraz DPC i M. Schrems, wymóg ten kontrastuje z orzecnictwem Trybunału, zgodnie z którym, aby stwierdzić, że doszło do ingerencji w prawo do poszanowania życia prywatnego danej osoby, bez znaczenia jest to, czy osoba ta doświadczyła ewentualnych niedogodności z powodu zarzucanej ingerencji²⁰³.

325. Poza tym nie przekonuje mnie wyrażone przez Facebook Ireland i rząd Stanów Zjednoczonych stanowisko, zgodnie z którym niedociągnięcia charakteryzujące ochronę sądową osób, których dane zostały przekazane do Stanów Zjednoczonych, miałyby być rekompensowane poprzez kontrole sprawowane przez FISC uprzednio i a posteriori, oraz poprzez liczne mechanizmy nadzoru ustanowione w ramach władzy wykonawczej i ustawodawczej²⁰⁴.

326. Jak już zauważyłem, po pierwsze, zgodnie z ustaleniami zawartymi w decyzji w sprawie Tarczy Prywatności, FISC nie kontroluje indywidualnych środków nadzorczych przed ich wdrożeniem²⁰⁵. Po drugie, jak wskazano w motywie 109 tej decyzji i co potwierdził rząd Stanów Zjednoczonych w udzielonej na piśmie odpowiedzi na pytania zadane przez Trybunał, przeprowadzana ex post kontrola stosowania selektorów ma na celu sprawdzenie przestrzegania przewidzianych w corocznej certyfikacji warunków dotyczących wyboru selektorów w przypadku, gdy FISC uzyska od agencji wywiadu informację o incydencie dotyczącym możliwego naruszenia procedur ukierunkowywania i minimalizacji²⁰⁶. W związku z tym nie wydaje się, aby postępowanie przed FISC stanowiło skuteczny środek indywidualnej ochrony prawnej dla osób, których dane są przekazywane do Stanów Zjednoczonych.

327. Chociaż pozasądowe mechanizmy kontroli wyszczególnione w motywach 95–110 decyzji w sprawie Tarczy Prywatności mogłyby w razie potrzeby wzmocnić inne możliwości zaskarżenia na drodze sądowej, to jednak w mojej ocenie, nie mogą one wystarczyć dla zapewnienia osobom, których dane dotyczą, odpowiedniego stopnia ochrony jeśli chodzi o prawo do wniesienia środka zaskarżenia. W szczególności wydaje się, że inspektorzy generalni należący do struktury wewnętrznej każdej agencji, nie stanowią niezależnego mechanizmu kontroli. Z kolei nadzór sprawowany przez PCLOB oraz przez komisje ds. wywiadu Kongresu nie jest równoznaczny z mechanizmem indywidualnego środka ochrony prawnej przed środkami nadzorczymi.

328. W związku z tym należy zbadać, czy instytucja rzecznika uzupełnia te luki zapewniając osobom, których dane dotyczą, skuteczny środek ochrony prawnej przed niezawisłym i bezstronnym organem²⁰⁷.

329. Po drugie, pragnę przypomnieć, że, aby ocenić ustalenia dotyczące adekwatności dokonane w decyzji w sprawie Tarczy Prywatności w kontekście środków ochrony prawnej przysługujących osobom, które uważają, iż były poddane nadzorowi na podstawie EO 12333, właściwymi ramami odniesienia są postanowienia EKPC.

203 Wyrok z dnia 20 maja 2003 r., Österreichischer Rundfunk i in. (sprawy połączone C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 75); wyrok Digital Rights Ireland (pkt 33); wyrok Schrems (pkt 87); opinia 1/15 (pkt 124).

204 Mechanizmy te są opisane w motywach 95–110 decyzji w sprawie Tarczy Prywatności. W motywach tych Komisja dokonuje w ramach kategorii zasad odnoszących się do „skutecznej ochrony prawnej” rozróżnienia na „mechanizmy nadzoru” (zob. motywy 92–110) i „dochodzenie roszczeń przez osoby fizyczne” (zob. motywy 111–124).

205 Zobacz pkt 298 niniejszej opinii.

206 Zgodnie z motywem 109 decyzji w sprawie Tarczy Prywatności „[p]rokurator Generalny i Dyrektor [NSA] weryfikują zgodność z zasadami, a agencje są zobowiązane do zgłaszania Sądowi ds. Inwigilacji Obcych Wywiadów (a także Kongresowi i prezydenckiej Radzie Nadzoru nad Służbami Wywiadowczymi) wszelkich przypadków nieprzestrzegania zasad – na tej podstawie Sąd może wprowadzić zmiany w upoważnieniu”.

207 Zobacz pkt 333–340 niniejszej opinii.

330. Jak poprzednio wskazałem²⁰⁸, ETPC oceniając, czy dany środek nadzorczy spełnia warunki przewidywalności i „niezbędności w społeczeństwie demokratycznym” w rozumieniu art. 8 ust. 2 EKPC²⁰⁹, bada całokształt mechanizmów kontroli i nadzoru wdrożonych „przed, podczas i po” zastosowaniu tego środka. W sytuacji, gdy przeszkodą w skorzystaniu z indywidualnego środka ochrony prawnej jest okoliczność, że zawiadomienie o zastosowaniu środka nadzorczego nie jest możliwe bez narażenia na szwank jego skuteczności²¹⁰, ta luka może być zrekompensowana przez wdrożenie niezależnej kontroli poprzedzającej zastosowanie rozpatrywanego środka²¹¹. W związku z tym ETPC nie nadaje takiemu zawiadomieniu rangi wymogu pomimo tego, że uznaje je za „pożądane”, o ile może ono nastąpić bez narażania na szwank skuteczności środka nadzorczego²¹².

331. Z decyzji w sprawie Tarczy Prywatności nie wynika w tym względzie, żeby osoby, których dane dotyczą, były zawiadamiane o środkach nadzorczych stosowanych na podstawie na EO 12333, ani też, że środki te miałyby podlegać opartym na zasadzie niezawisłości mechanizmom kontroli sądowej lub administracyjnej na jakimkolwiek etapie ich przyjmowania lub wdrażania.

332. W tych okolicznościach należy zbadać, czy instytucja skargi do rzecznika umożliwia jednak zapewnienie niezależnej kontroli środków nadzorczych, w tym tych opartych na EO 12333.

2) W przedmiocie wpływu mechanizmu mediacji na stopień ochrony prawa do skutecznego środka ochrony prawnej

333. Zgodnie z motywem 116 decyzji w sprawie Tarczy Prywatności mechanizm mediacji opisany w załączniku III A do tej decyzji ma na celu ustanowienie dodatkowych środków zaskarżenia osobom, których dane są przekazywane z Unii do Stanów Zjednoczonych.

334. Jak zaznaczył rząd Stanów Zjednoczonych, dopuszczalność wniesienia skargi do rzecznika nie jest uzależniona od spełnienia wymogów dotyczących legitymacji procesowej podobnych do tych, które regulują dostęp do amerykańskich sądów. W motywie 119 rzeczony decyzji wyjaśniono w tym względzie, że dla wniesienia skargi do rzecznika nie jest wymagane, aby zainteresowana osoba wykazywała, iż rząd amerykański pozyskał dotyczące jej dane osobowe.

335. Podobnie jak DPC, M. Schrems, rządy polski i portugalski oraz EPIC, mam wątpliwości, co do tego, czy mechanizm ten jest zdolny zrekompensować braki ochrony sądowej oferowanej osobom, których dane są przekazywane z Unii do Stanów Zjednoczonych.

²⁰⁸ Zobacz pkt 305 niniejszej opinii.

²⁰⁹ ETPC w swoim orzecznictwie dotyczącym środków nadzorczych stosowanych w telekomunikacji rozpatrywał kwestię środków ochrony prawnej w ramach badania „jakości prawa” i konieczności ingerencji w korzystanie z prawa zagwarantowanego w art. 8 EKPC [zob. w szczególności wyroki Zakharov (§ 236) i Centrüm för Rättvisa (§ 107)]. ETPC w wyroku z dnia 1 lipca 2008 r., Liberty i in. przeciwko Zjednoczonemu Królestwu (CE:ECHR:2008:0701JUD005824300, § 73), oraz w wyroku Zakharov (§ 307), stwierdziwszy naruszenie art. 8 EKPC, nie uznał za konieczne przeprowadzania odrębnego badania zarzutu dotyczącego naruszenia art. 13 tej konwencji.

²¹⁰ Zdaniem ETPC, o ile brak zawiadomienia na którymkolwiek z etapów nie zawsze uniemożliwia spełnienie przez środek nadzorczy warunku „niezbędności w społeczeństwie demokratycznym”, to brak ten zagraża dostępowi do sądów, a tym samym skuteczności środków ochrony prawnej [zob. w szczególności wyrok z dnia 6 września 1978 r., Klass i in. przeciwko Niemcom (CE:ECHR:1978:0906JUD000502971, § 57 i 58); rozstrzygnięcie Weber i Saravia (§ 135), i wyrok Zakharov (§ 302)].

²¹¹ Zobacz podobnie wyrok Centrüm för Rättvisa (§ 105).

²¹² W wyroku Big Brother Watch (§ 317) ETPC odmówił zaliczenia do minimalnych zabezpieczeń mających zastosowanie do systemu inwigilacji charakteryzującego się masowym przechwytywaniem komunikatów elektronicznych, wymogu, aby osoby których dane dotyczą, były zawiadamiane o inwigilacji. Zobacz również wyrok Centrüm för Rättvisa (§ 164). Przekazanie tych wyroków do wielkiej izby ETPC ma na celu między innymi ponowne zbadanie tego wniosku.

336. Przede wszystkim, pomimo tego, że mechanizm pozasądowych środków ochrony prawnej może stanowić skuteczny środek prawny w rozumieniu art. 47 TFUE, jest tak wyłącznie w przypadku, gdy rozpatrywany organ ma umocowanie ustawowe i spełnia warunek niezawisłości²¹³.

337. Z decyzji w sprawie Tarczy Prywatności wynika, że mechanizm mediacji, którego źródłem jest PPD 28²¹⁴, nie ma umocowania ustawowego. Rzecznik jest wyznaczany przez Sekretarza Stanu i stanowi integralną część Departamentu Stanu Stanów Zjednoczonych²¹⁵. W decyzji tej nie zawarto żadnego elementu mogącego świadczyć o tym, że odwołanie rzecznika lub stwierdzenie nieważności jego mianowania podlega szczególnym gwarancjom²¹⁶. Mimo że rzecznik jest przedstawiany jako niezależny od „wspólnoty wywiadowczej”, ponosi on odpowiedzialność przed Sekretarzem Stanu i, co za tym idzie, nie jest niezależny od władzy ustawodawczej²¹⁷.

338. Następnie, skuteczność pozasądowego środka ochrony prawnej zależy również, jak się wydaje, od posiadania przez ten organ możliwości wydawania wiążących i uzasadnionych orzeczeń. Jeśli chodzi o tę kwestię, decyzja w sprawie Tarczy Prywatności nie zawiera żadnego elementu świadczącego o tym, że rzecznikowi miałyby przysługiwać uprawnienie do wydawania takich orzeczeń. W decyzji tej nie wykazano, że instytucja rzecznika umożliwia skarżącemu uzyskanie dostępu do dotyczących ich danych, nakazanie ich sprostowania lub usunięcia, ani też, że rzecznik miałby przyznawać odszkodowanie osobom pokrzywdzonym w wyniku zastosowania wobec nich środków nadzoru. W szczególności, jak wynika z załącznika III A pkt 4 lit. e) tej decyzji, „rzecznik [...] nie potwierdzi, ani nie zaprzeczy, że dana osoba jest objęta obserwacją [nadzorem], ani nie potwierdzi, że zastosowano specjalne środki zaradcze”²¹⁸. Choć rząd amerykański zobowiązał się do zapewnienia tego, że dana jednostka służb wywiadowczych będzie musiała podjąć działania naprawcze w związku z wszelkimi wykrytymi przez rzecznika naruszeniami obowiązujących przepisów²¹⁹, rzeczona decyzja nie wspomina o zabezpieczeniach prawnych, które towarzyszą temu zobowiązaniu i na które mogłyby się powoływać jednostki.

339. W związku z tym instytucja mediatora moim zdaniem nie zapewnia sprawowanej przez niezależny organ ochrony prawnej umożliwiającej osobom, których dane są przekazywane, dochodzenie przysługujących im praw do uzyskania dostępu do danych lub kwestionowanie uchybień obowiązującym zasadom, których miały dopuścić się służby wywiadowcze.

213 Pojęcie niezawisłości obejmuje aspekt pierwszy, o charakterze zewnętrznym, który zakłada ochronę organu przed ingerencją i naciskami zewnętrznymi mogącymi zagrozić niezależności osądu jego członków przy rozpatrywaniu przez nich sporów. Drugi aspekt tego pojęcia, wewnętrzny, łączy się z pojęciem „bezbtronności” i dotyczy jednakowego dystansu do stron sporu i ich odpowiednich interesów w odniesieniu do jego przedmiotu. Zobacz w szczególności wyroki: z dnia 19 września 2006 r., Wilson (C-506/04, EU:C:2006:587, pkt 50–52); z dnia 14 czerwca 2017 r., Online Games i in. (C-685/15, EU:C:2017:452, pkt 60, 61); z dnia 25 lipca 2018 r., Minister for Justice and Equality (Nieprawidłowości w systemie sądownictwa) (C-216/18 PPU, EU:C:2018:586, pkt 63, 65); z dnia 19 listopada 2019 r., A.K. i in. (Niezależność Izby Dyscyplinarnej Sądu Najwyższego) (C-585/18, C-624/18 i C-625/18, EU:C:2019:982, pkt 121, 122). Zgodnie z zasadą rozdziału władzy należy zagwarantować niezależność sądów, w szczególności w odniesieniu do władzy wykonawczej. Zob. wyrok z dnia 19 listopada 2019 r., A.K. i in. (Niezależność Izby Dyscyplinarnej Sądu Najwyższego) (C-585/18, C-624/18 i C-625/18, EU:C:2019:982, pkt 127 i przytoczone tam orzecznictwo).

214 W załączniku III A do decyzji w sprawie Tarczy Prywatności wskazano w tym względzie na sekcję 4 lit. d) PPD 28.

215 Zobacz motyw 116 decyzji w sprawie Tarczy Prywatności.

216 W wyroku z dnia 31 maja 2005 r., Syfait i in. (C-53/03, EU:C:2005:333, pkt 31), Trybunał podkreślił znaczenie takich gwarancji dla spełnienia warunku niezawisłości. Zobacz również w tym względzie wyroki z dnia 24 czerwca 2019 r., Komisja/Polska (Niezależność Sądu Najwyższego) (C-619/18, EU:C:2019:531, pkt 76) i z dnia 5 listopada 2019 r., Niezależność sądów powszechnych (C-192/18, EU:C:2019:924, pkt 113).

217 Zobacz motywy 65 i 121 oraz załącznik III A pkt 1 decyzji w sprawie Tarczy Prywatności.

218 Poza tym w motywie 121 decyzji w sprawie Tarczy Prywatności wskazano, że „[r]zecznik będzie musiał »potwierdzić«, iż (i) skarga została właściwie zbadana oraz że (ii) przestrzegano odpowiednich przepisów prawa amerykańskiego – w tym przede wszystkim ograniczeń i gwarancji opisanych w załączniku VI – lub – w przypadku nieprzestrzegania przepisów – problem ten został rozwiązany”.

219 W ramach trzeciego rocznego przeglądu funkcjonowania Tarczy Prywatności, Komisja stwierdziła, że zgodnie z deklaracjami rządu Stanów Zjednoczonych, w przypadku gdyby prowadzone przez rzecznika dochodzenie ujawniło naruszenie procedur ukierunkowywania i minimalizacji zatwierdzonych przez FISC, naruszenie takie zostanie zgłoszone temu sądowi. FISC dokona wówczas niezależnego przeglądu i, w stosownych przypadkach, zarządzi, aby właściwa agencja wywiadowcza podjęła działania naprawcze w związku z rzeczoną naruszeniem. Zobacz Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, 23 października 2019 r., SWD(2019) 390 final, s. 28. Komisja odnosi się w nim do dokumentu zatytułowanego »Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure«, dostępnego pod adresem <https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf> (s. 4 i 5).

340. Wreszcie, zgodnie z orzecznictwem, poszanowanie prawa gwarantowanego przez art. 47 karty wymagałoby wówczas, aby decyzja organu administracji, który sam nie spełnia wymogu niezawisłości, została poddana późniejszej kontroli przez organ sądowy, który powinien być właściwy w zakresie rozstrzygania każdej istotnej kwestii²²⁰. Tymczasem z wyjaśnień udzielonych w decyzji w sprawie Tarczy Prywatności wynika, że decyzje rzecznika nie są przedmiotem kontroli sprawowanej przez niezawisły sąd.

341. W tych okolicznościach, jak zauważyli DPC, M. Schrems, EPIC oraz rządy polski i portugalski, merytoryczna równowaga między ochroną sądową, jaka jest zapewniana w porządku prawnym Stanów Zjednoczonych osobom, których dane są przekazywane z Unii do tego państwa, a ochroną sądową wynikającą z RODO w związku z art. 47 karty i art. 8 EKPC, wydaje się być wątpliwa.

342. W świetle całości powyższych rozważań mam pewne wątpliwości co do zgodności decyzji w sprawie Tarczy Prywatności z art. 45 ust. 1 RODO w związku z art. 7, 8 i 47 karty oraz art. 8 EKPC.

V. Wnioski

343. Proponuję, aby Trybunał udzielił następującej odpowiedzi na pytania prejudycjalne przedłożone przez High Court (wysoki trybunał, Irlandia):

Analiza pytań prejudycjalnych nie doprowadziła do ujawnienia jakiegokolwiek okoliczności, która mogłaby wpływać na ważność decyzji 2010/87/UE z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, zmienionej decyzją wykonawczą Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r.

²²⁰ Zobacz wyroki z dnia 16 maja 2017 r., *Berlioz Investment Fund* (C-682/15, EU:C:2017:373, pkt 55); z dnia 13 grudnia 2017 r., *El Hassani* (C-403/16, EU:C:2017:960, pkt 39).