WYROK TRYBUNAŁU (wielka izba)

z dnia 6 października 2015 r.

Odesłanie prejudycjalne – Dane osobowe – Ochrona osób fizycznych w zakresie przetwarzania tych danych – Karta praw podstawowych Unii Europejskiej – Artykuły 7, 8 i 47 – Dyrektywa 95/46/WE – Artykuły 25 i 28 – Przekazywanie danych osobowych do państw trzecich – Decyzja 2000/520/WE – Przekazywanie danych osobowych do Stanów Zjednoczonych – Nieodpowiedni stopień ochrony – Ważność – Skarga osoby fizycznej, której dane zostały przekazane z Unii Europejskiej do Stanów Zjednoczonych – Kompetencje krajowych organów nadzorczych

W sprawie C-362/14

mającej za przedmiot wniosek o wydanie, na podstawie art. 267 TFUE, orzeczenia w trybie prejudycjalnym, złożony przez High Court (Irlandia) postanowieniem z dnia 17 lipca 2014 r., które wpłynęło do Trybunału w dniu 25 lipca 2014 r., w postępowaniu:

Maximillian Schrems

przeciwko

Data Protection Commissioner,

przy udziale:

Digital Rights Ireland Ltd,

TRYBUNAŁ (wielka izba),

w składzie: V. Skouris, prezes, K. Lenaerts, wiceprezes, A. Tizzano, R. Silva de Lapuerta, T. von Danwitz (sprawozdawca), S. Rodin i K. Jürimäe, prezesi izb, A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M. Berger, F. Biltgen i C. Lycourgos, sędziowie,

rzecznik generalny: Y. Bot,

sekretarz: L. Hewlett, główny administrator,

uwzględniając pisemny etap postępowania i po przeprowadzeniu rozprawy w dniu 24 marca 2015 r.,

rozważywszy uwagi przedstawione:

– w imieniu M. Schremsa przez N. Traversa, SC, P. O'Shea, BL, G. Ruddena, solicitor, oraz H. Hofmanna, Rechtsanwalt,

– w imieniu Data Protection Commissioner przez P. McDermotta, BL, S. More-O'Ferrall oraz D. Younga, solicitors,

– w imieniu Digital Rights Ireland Ltd przez F. Crehana, BL, S. McGarra oraz E. McGarra, solicitors,

– w imieniu Irlandii przez A. Joyce'a, B. Counihana oraz E. Creedon, działających w charakterze pełnomocników, wspieranych przez D. Fennelly'ego, BL,

– w imieniu rządu belgijskiego przez J.C. Halleux oraz C. Pochet, działających w charakterze pełnomocników,

– w imieniu rządu czeskiego przez M. Smolka oraz J. Vláčila, działających w charakterze pełnomocników,

– w imieniu rządu włoskiego przez G. Palmieri, działającą w charakterze pełnomocnika, wspieraną przez P. Gentilego, avvocato dello Stato,

– w imieniu rządu austriackiego przez G. Hessego oraz G. Kunnerta, działających w charakterze pełnomocników,

– w imieniu rządu polskiego przez M. Kamejszę, M. Pawlicką oraz B. Majczynę, działających w charakterze pełnomocników,

– w imieniu rządu słoweńskiego przez A. Grum oraz V. Klemenc, działające w charakterze pełnomocników,

– w imieniu rządu Zjednoczonego Królestwa przez L. Christiego oraz J. Beeko, działających w charakterze pełnomocników, wspieranych przez J. Holmesa, barrister,

– w imieniu Parlamentu Europejskiego przez D. Moore'a, A. Caiolę oraz M. Penchevę, działających w charakterze pełnomocników,

– w imieniu Komisji Europejskiej przez B. Schimę, B. Martenczuka, B. Smuldersa oraz J. Vondung, działających w charakterze pełnomocników,

– w imieniu Europejskiego Inspektora Ochrony Danych (EIOD) przez C. Dockseya, A. Buchtę oraz V. Péreza Asinariego, działających w charakterze pełnomocników,

po zapoznaniu się z opinią rzecznika generalnego na posiedzeniu w dniu 23 września 2015 r.,

wydaje następujący

Wyrok

1 Wniosek o wydanie orzeczenia w trybie prejudycjalnym dotyczy wykładni – w świetle art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej „kartą") – art. 25 ust. 6 i art. 28 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281, s. 31 – wyd. spec. w jęz. polskim, rozdz. 13, t. 15, s. 355), zmienionej rozporządzeniem (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. (Dz.U. L 284, s. 1 – wyd. spec. w jęz. polskim, rozdz. 1, t. 4, s. 447) (zwanej dalej „dyrektywą 95/46"), a także – w istocie –

ważności decyzji Komisji 2000/520/WE z dnia 26 lipca 2000 r., przyjętej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA (Dz.U. L 215, s. 7 – wyd. spec. w jęz. polskim, rozdz. 16, t. 1, s. 119).

2 Wniosek ten został złożony w ramach postępowania w sprawie sporu pomiędzy M. Schremsem a Data Protection Commissioner (komisarzem ds. ochrony danych, zwanym dalej „komisarzem") dotyczącego odmowy rozpatrzenia przez komisarza skargi wniesionej przez M. Schremsa z powodu przekazywania przez Facebook Ireland Ltd (zwaną dalej „Facebook Ireland" lub „spółką Facebook Ireland") do Stanów Zjednoczonych danych osobowych swoich użytkowników i przechowywania owych danych na serwerach położonych w tym państwie.

Ramy prawne

Dyrektywa 95/46

3 Motywy 2, 10, 56, 57, 60, 62 i 63 dyrektywy 95/46 mają następujące brzmienie:

„(2) Systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi; muszą one, niezależnie od obywatelstwa czy miejsca stałego zamieszkania osób fizycznych, szanować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do […] dobrobytu jednostek.

[…]

(10) Celem krajowych przepisów prawa dotyczących przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności [podpisanej w Rzymie dnia 4 listopada 1950 r.] oraz w zasadach ogólnych prawa wspólnotowego; z tego powodu zbliżanie przepisów prawa nie powinno wpłynąć na zmniejszenie ochrony, jaką gwarantują, lecz przeciwnie, musi dążyć do zapewnienia jak najwyższego stopnia ochrony we Wspólnocie.

[…]

(56) Transgraniczny przepływ danych osobowych jest koniecznym warunkiem rozwoju handlu międzynarodowego; ochrona osób, jaką niniejsza dyrektywa gwarantuje we Wspólnocie, nie stanowi przeszkody dla przekazywania danych osobowych do państw trzecich, które zapewniają odpowiedni stopień ochrony; prawidłowość [odpowiedniość] stopnia ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazywania danych lub zestawu takich operacji.

(57) Z drugiej strony należy zakazać przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony.

[…]

(60) W każdym przypadku przekazywanie danych do państw trzecich może następować jedynie w pełnej zgodności z przepisami przyjętymi przez państwa członkowskie na podstawie niniejszej dyrektywy, w szczególności jej art. 8.

[…]

(62) Utworzenie w państwach członkowskich organów nadzorczych, wykonujących swoje funkcje w sposób całkowicie niezależny jest zasadniczym elementem ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

(63) Organy te muszą dysponować określonymi środkami do realizacji swoich obowiązków, włączając uprawnienia do przeprowadzania dochodzenia i interwencji, szczególnie w przypadkach skarg od obywateli, jak również uprawnienia do brania udziału w postępowaniu sądowym […]".

4 Artykuły 1, 2, 25, 26, 28 i 31 dyrektywy 95/46 stanowią:

„Artykuł 1

Cel dyrektywy

1. Zgodnie z przepisami niniejszej dyrektywy, państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych.

[…]

Artykuł 2

Definicje

Do celów niniejszej dyrektywy:

a) »dane osobowe« oznacza[ją] wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (»osoby, której dane dotyczą«); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość;

b) »przetwarzanie danych osobowych« (»przetwarzanie«) oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie;

[…]

d) »administrator danych« oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określane w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalane przez ustawodawstwo krajowe lub wspólnotowe;

[…]

Artykuł 25

Zasady

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.

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.

3. Państwa członkowskie i Komisja będą informować się wzajemnie o przypadkach, kiedy uznają, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2.

4. Jeżeli Komisja stwierdzi, na podstawie procedury przewidzianej w art. 31 ust. 2, że państwo trzecie nie zapewnia odpowiedniego stopnia ochrony w znaczeniu ust. 2 niniejszego artykułu, państwa członkowskie podejmą konieczne środki, aby nie dopuścić do przekazania jakichkolwiek danych tego samego rodzaju do wspomnianego państwa trzeciego.

5. We właściwym czasie Komisja przystąpi do negocjacji w celu zaradzenia sytuacji stwierdzonej na podstawie ust. 4.

6. Komisja może stwierdzić, zgodnie z procedurą określoną w art. 31 ust. 2, że państwo trzecie zapewnia prawidłowy [odpowiedni] 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.

Artykuł 26

Odstępstwa

1. W drodze odstępstwa od przepisów art. 25 oraz, z zastrzeżeniem odmiennych przepisów prawa krajowego dotyczącego konkretnych przypadków, państwa członkowskie zapewnią, że przekazanie lub przekazywanie danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony w znaczeniu art. 25 ust. 2 może nastąpić pod warunkiem że:

a) osoba, której dane dotyczą, jednoznacznie udzieli zgody na proponowane przekazanie danych; lub

b) przekazanie danych jest konieczne dla realizacji umowy między osobą, której dane dotyczą i administratorem danych lub dla wprowadzenia w życie ustaleń poprzedzających zawarcie umowy na wniosek osoby, której dane dotyczą; lub

c) przekazanie danych jest konieczne dla zawarcia lub wykonania umowy zawartej między administratorem danych i osobą trzecią, w interesie osoby, której dane dotyczą, lub

d) przekazanie danych jest konieczne lub wymagane przez prawo z ważnych względów publicznych [interesu publicznego] lub w celu ustanowienia, wykonania lub obrony tytułu prawnego; lub

e) przekazanie danych jest konieczne dla zapewnienia ochrony żywotnych interesów osoby, której dane dotyczą; lub

f) przekazanie danych następuje z rejestru, który ma służyć, zgodnie z obowiązującymi przepisami ustawowymi lub wykonawczymi, za źródło informacji dla ogółu społeczeństwa, udostępnionego do konsultacji obywateli i każdej osoby wykazującej uzasadniony interes, o ile warunki określone przez prawo odnośnie do wglądu do takiego rejestru zostały w danym przypadku spełnione.

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.

3. Państwo członkowskie powiadamia Komisję i inne państwa członkowskie o upoważnieniach wydanych na podstawie ust. 2.

Jeżeli państwo członkowskie lub Komisja zgłaszają sprzeciw w oparciu o uzasadnione przyczyny związane z ochroną prywatności oraz podstawowych praw i wolności osób fizycznych, Komisja podejmuje właściwe środki zgodnie z procedurą określoną w art. 31 ust. 2.

Państwa członkowskie podejmą konieczne środki w celu zastosowania się do decyzji Komisji.

[…]

Artykuł 28

Organ nadzorczy

1. Każde państwo członkowskie zapewni, że jeden lub więcej organów władzy publicznej będzie odpowiedzialnych za kontrolę stosowania na jego terytorium przepisów przyjętych przez państwa członkowskie na mocy niniejszej dyrektywy.

Organy te postępują w sposób całkowicie niezależny przy wykonywaniu powierzonych im funkcji.

2. Każde państwo członkowskie wprowadza obowiązek konsultowania się z organami nadzorczymi przy opracowywaniu środków administracyjnych lub przepisów dotyczących ochrony praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych.

3. Każdy organ jest w szczególności wyposażony w:

– uprawienia dochodzeniowe, jak np. prawo dostępu do danych stanowiących przedmiot operacji przetwarzania danych oraz prawo gromadzenia wszelkich informacji potrzebnych do wykonywania jego funkcji nadzorczych,

– 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,

– prawo pozywania w przypadku naruszenia krajowych przepisów przyjętych zgodnie z niniejszą dyrektywą lub powiadomienie organów sądowych o takim naruszeniu.

Od decyzji organu nadzorczego, co do którego zgłaszane są zastrzeżenia [Od niekorzystnej decyzji organu nadzorczego], przysługuje odwołanie do właściwego sądu.

4. Każdy organ nadzorczy rozpatruje skargi zgłaszane przez dowolną osobę lub przez stowarzyszenie ją reprezentujące, odnośnie do ochrony jej praw i wolności w zakresie przetwarzania danych osobowych. Zainteresowana osoba zostanie poinformowana o wyniku sprawy.

Każdy organ nadzorczy w szczególności rozpatruje skargi dotyczące kontroli legalności przetwarzania danych, zgłaszane przez dowolną osobę, kiedy mają zastosowanie krajowe przepisy przyjęte zgodnie z art. 13 niniejszej dyrektywy. Osoba ta zostanie w każdym przypadku poinformowana o przeprowadzeniu kontroli.

[…]

6. Każdy organ nadzorczy jest właściwy, niezależnie od krajowych przepisów dotyczących danego przypadku przetwarzania danych, do wykonywania na terytorium państwa członkowskiego uprawnień powierzonych mu zgodnie z ust. 3. Do każdego organu można się zwrócić z żądaniem wykonania jego uprawnień przez odpowiedni organ innego państwa członkowskiego.

[…]

Artykuł 31

[…]

2. W przypadku odniesienia się do niniejszego artykułu – art. 4 i 7 decyzji [Rady] 1999/468/WE [z dnia 28 czerwca 1999 r. ustanawiającej warunki wykonywania uprawnień wykonawczych przyznanych Komisji (Dz.U. L 184, s. 23)] stosuje się z uwagi na przepisy zawarte w jej art. 8.

[…]".

Decyzja 2000/520

5 Komisja przyjęła decyzję 2000/520 na podstawie art. 25 ust. 6 dyrektywy 95/46.

6 Motywy 2, 5 i 8 tej decyzji brzmią następująco:

„(2) Komisja może stwierdzić, że państwo trzecie zapewnia adekwatny [odpowiedni] poziom bezpieczeństwa [ochrony]. W tym przypadku dane osobowe mogą być przekazywane z państw członkowskich bez konieczności dodatkowych gwarancji.

[…]

(5) Adekwatny [Odpowiedni] poziom ochrony przekazywania danych ze Wspólnoty do Stanów Zjednoczonych, uznany przez niniejszą decyzję [na podstawie niniejszej decyzji], powinien zostać osiągnięty, jeżeli organizacje będą przestrzegać zasad ochrony prywatności w ramach »bezpiecznej przystani« dotyczących ochrony danych osobowych przekazywanych z państwa członkowskiego do Stanów Zjednoczonych (zwanych dalej »zasadami«) i najczęściej zadawanych pytań (zwanych dalej »NZP«), zawierających wytyczne dotyczące wprowadzania w życie zasad wydanych przez Rząd Stanów Zjednoczonych w dniu 21 lipca 2000 r. Ponadto organizacje powinny publicznie ujawnić stosowane przez nie polityki ochrony prywatności, a także powinny zostać poddane bądź to właściwości [Federal Trade Commission] (Federalnej Komisji Handlu (FKH)] na podstawie sekcji 5 ustawy o Federalnej Komisji Handlu, która zakazuje nieuczciwych lub wprowadzających w błąd czynów bądź praktyk handlowych lub wpływających na handel, bądź innego ustawowego organu, który skutecznie zapewni przestrzeganie zasad wdrożonych zgodnie z NZP.

[…]

(8) Dla zachowania przejrzystości i w celu zagwarantowania właściwym władzom w państwach członkowskich możliwości zapewnienia ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych, konieczne jest wyszczególnienie w niniejszej decyzji okoliczności wyjątkowych, w których zawieszenie określonych przekazów danych powinno być usprawiedliwione, bez względu na to czy stwierdzono ich właściwą ochronę".

7 Zgodnie z art. 1–4 decyzji 2000/520:

„Artykuł 1

1. Do celów art. 25 ust. 2 dyrektywy 95/46/WE, w odniesieniu do wszystkich działań wchodzących w zakres niniejszej dyrektywy przyjmuje się, że zasady ochrony prywatności w ramach »bezpiecznej przystani« (zwane dalej »zasadami«), jak określono w załączniku I do niniejszej decyzji, wprowadzane w życie zgodnie z wytycznymi zawartymi w najczęściej zadawanych pytaniach (zwanych dalej »NZP«) wydanych przez Departament Handlu USA w dniu 21 lipca 2000 r., jak określono w załączniku II do niniejszej decyzji, zapewniają adekwatny [odpowiedni] poziom ochrony danych osobowych przekazywanych ze Wspólnoty do organizacji mających siedzibę w Stanach Zjednoczonych, z uwzględnieniem następujących dokumentów wydanych przez Departament Handlu USA:

a) przegląd egzekwowania »bezpiecznej przystani«, przedstawiony w załączniku III;

b) memorandum w sprawie odszkodowań z tytułu naruszenia prywatności i wyraźnych upoważnień w prawie amerykańskim, przedstawione w załączniku IV;

c) list Federalnej Komisji Handlu, przedstawiony w załączniku V;

d) list Departamentu Transportu USA, przedstawiony w załączniku VI.

2. W stosunku do każdego przekazu danych powinny zostać spełnione następujące warunki:

a) organizacja otrzymująca dane jednoznacznie i publicznie ujawniła swoje zobowiązanie przestrzegania zasad wdrożonych zgodnie z NZP; oraz

b) organizacja podlega ustawowym uprawnieniom organu rządowego Stanów Zjednoczonych wymienionego w załączniku VII do niniejszej decyzji, który w przypadku nieprzestrzegania zasad wdrożonych przy pomocy NZP jest upoważniony do badania skarg i uwalniania od nieuczciwych lub wprowadzających w błąd praktyk oraz uzyskiwania odszkodowania dla osób fizycznych, niezależnie od ich kraju zamieszkania bądź przynależności państwowej.

3. Przyjmuje się, że warunki określone w ust. 2 spełnia każda organizacja, która deklaruje przestrzeganie zasad wdrożonych zgodnie z NZP od dnia, w którym ta organizacja zawiadomi Departament Handlu USA (albo osobę przez niego wyznaczoną) o publicznym ujawnieniu zobowiązania określonego w ust. 2 lit. a) oraz danych organu rządowego, określonego w ust. 2 lit. b).

Artykuł 2

Niniejsza decyzja dotyczy jedynie adekwatności [odpowiedniego stopnia] ochrony zapewnianej w Stanach Zjednoczonych na mocy zasad wdrożonych zgodnie z NZP w celu spełnienia wymagań art. 25 ust. 1 dyrektywy 95/46/WE i nie wpływa na stosowanie innych przepisów tej dyrektywy, które dotyczą przetwarzania danych osobowych w państwach członkowskich, w szczególności jej art. 4.

Artykuł 3

1. Bez uszczerbku dla ich uprawnień do podejmowania działania zmierzającego do zapewnienia zgodności z przepisami krajowymi przyjętymi na mocy przepisów innych niż

art. 25 dyrektywy 95/46/WE, właściwe władze państw członkowskich mogą wykonywać posiadane uprawnienia w celu zawieszenia przepływu danych do organizacji, która złożyła zaświadczenie o przestrzeganiu zasad wdrożonych zgodnie z NZP, w celu ochrony osób fizycznych w odniesieniu do przetwarzania ich danych osobowych w przypadkach, gdy:

a) organ rządowy w Stanach Zjednoczonych, określony w załączniku VII do niniejszej decyzji lub mechanizm niezależnej ochrony prawnej w rozumieniu lit. a) Zasady Realizacji Prawa określonej w załączniku I do niniejszej decyzji ustali, że organizacja narusza zasady wdrożone zgodnie z NZP; lub

b) istnieje duże prawdopodobieństwo, że zasady są łamane; istnieje uzasadnione domniemanie, że mechanizm realizacji prawa, o którym mowa, nie podejmuje lub nie podejmie właściwych kroków w odpowiednim czasie w celu załatwienia spornej sprawy; dalszy przekaz tworzyłby bezpośrednie ryzyko wystąpienia poważnej szkody dla osób, których dane dotyczą; a właściwe władze państwa członkowskiego dołożyły należytych starań w tych okolicznościach w celu powiadomienia danej organizacji i umożliwienia udzielenia odpowiedzi.

Zawieszenie ustaje z chwilą, gdy zostanie zapewnione przestrzeganie zasad wdrożonych zgodnie z NZP oraz właściwe władze Wspólnoty zostaną o tym powiadomione.

2. Państwa członkowskie bezzwłocznie powiadomią Komisję o przyjęciu środków na podstawie ust. 1.

3. Państwa członkowskie i Komisja powiadomią się także o przypadkach, w których działanie organów odpowiedzialnych za zapewnienie przestrzegania zasad wdrożonych zgodnie z NZP w Stanach Zjednoczonych nie zapewnia ich przestrzegania.

4. Jeżeli informacje zebrane zgodnie z ust. 1, 2 i 3 dostarczą dowodów, że jakikolwiek organ odpowiedzialny za zapewnienie przestrzegania zasad wdrożonych zgodnie z NZP w Stanach Zjednoczonych nie spełnia skutecznie swojej roli, Komisja informuje o tym Departament Handlu USA oraz, w razie potrzeby, przedstawia projekt środków zgodnie z procedurą, określoną w art. 31 dyrektywy 95/46/WE, w celu uchylenia albo zawieszenia niniejszej decyzji lub też ograniczenia jej zakresu.

Artykuł 4

1. Niniejsza decyzja może być dostosowywana w dowolnym czasie w świetle doświadczenia uzyskanego podczas wprowadzania jej w życie i/lub, jeżeli wymagania ustawodawstwa USA będą wyższe niż poziom bezpieczeństwa [ochrony] zapewniany przez zasady i NZP.

W każdym przypadku, Komisja oceni wprowadzanie w życie niniejszej decyzji na podstawie dostępnych informacji trzy lata od jej notyfikowania państwom członkowskim i złoży sprawozdanie na temat wszelkich stosownych ustaleń komitetowi, ustanowionemu na podstawie art. 31 dyrektywy 95/46/WE, łącznie z wszelkimi dowodami, które mogą wpływać na ocenę przepisów określonych w art. 1 niniejszej decyzji w odniesieniu do zapewniania przez nie właściwej ochrony w rozumieniu art. 25 dyrektywy 95/46/WE oraz wszelkimi dowodami na stosowanie praktyk dyskryminacyjnych przy wprowadzaniu w życie niniejszej decyzji.

2. Komisja, w miarę potrzeb, przedstawia projekt środków zgodnie z procedurą określoną w art. 31 dyrektywy 95/46/WE”.

8 Załącznik I do decyzji 2000/520 stanowi, co następuje:

„Zasady ochrony prywatności w ramach »bezpiecznej przystani« wydane przez Departament Handlu USA dnia 21 lipca 2000 r.

[…]

[…] Departament Handlu wydaje niniejszy dokument i najczęściej zadawane pytania (zwane dalej »zasadami«) na mocy swych ustawowych uprawnień do ustanawiania, wspierania i rozwijania handlu międzynarodowego. Zasady zostały opracowane w konsultacji z kręgami przemysłowymi i publicznością [szeroką opinią publiczną] w celu ułatwienia handlu między Stanami Zjednoczonymi a Unią Europejską. Są one przeznaczone do wyłącznego użytku przez amerykańskie organizacje otrzymujące dane osobowe z Unii Europejskiej, w celu zakwalifikowania ich jako »bezpiecznej przystani« i domniemania »adekwatności [odpowiedniego stopnia ochrony]«, jakie ta przystań stwarza. Ponieważ zasady miały służyć wyłącznie temu szczególnemu celowi, ich przyjęcie do innych celów może być niewłaściwe […].

Decyzje organizacji o zakwalifikowaniu się jako »bezpieczna przystań« są całkowicie dobrowolne i organizacje mogą kwalifikować się jako »bezpieczna przystań« w różny sposób […].

Przyjęcie zasad może być ograniczone: a) w zakresie niezbędnym do spełnienia wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa; b) ustawą, rozporządzeniem rządu albo prawem precedensowym, ustanawiającym sprzeczne obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie; lub c) jeżeli efektem dyrektywy w prawie państwa członkowskiego jest dopuszczenie wyjątków lub odstępstw, pod warunkiem że takie wyjątki lub odstępstwa stosuje się w porównywalnych kontekstach. Zgodnie z celem zwiększenia ochrony prywatności, organizacje powinny dążyć do pełnego wdrożenia niniejszych zasad w sposób całkowity i przejrzysty, wskazując ponadto w swoich politykach ochrony prywatności przypadki, w których wyjątki od zasad dozwolone lit. b) powyżej będą stosowane na bieżąco. Z tego samego powodu w przypadku gdy zasady i/lub prawo amerykańskie dopuszcza taką możliwość, oczekuje się, że w miarę możliwości organizacje będą decydować się na wyższy poziom ochrony.

[…]”.

9 Załącznik II do decyzji 2000/520 ma następujące brzmienie:

„Najczęściej zadawane pytania (NZP)

[…]

NZP 6 – Samocertyfikacja

P: W jaki sposób organizacja może przedstawić [wydany przez siebie] certyfikat, że przystępuje do zasad »bezpiecznej przystani«?

O: Przywileje »bezpiecznej przystani« przysługują od dnia, w którym organizacja przedstawia swój [wydany przez siebie] certyfikat w [amerykańskim] Departamencie Handlu (albo u osoby przez niego wyznaczonej) zaświadczający, że będzie przestrzegać zasad zgodnie z instrukcjami podanymi poniżej.

W celu dokonania samocertyfikacji o przystąpieniu do »bezpiecznej przystani« organizacje mogą dostarczyć do [amerykańskiego] Departamentu Handlu (albo osoby przez niego wyznaczonej) list podpisany przez członka zarządu w imieniu organizacji, która przystępuje do »bezpiecznej przystani«, zawierający, co najmniej następujące informacje:

1. nazwę organizacji, adres pocztowy, adres e-mail, numery telefonu i faksu;

2. opis działalności organizacji w odniesieniu do informacji osobowych otrzymywanych z UE; oraz

3. opis obowiązującej w organizacji polityki ochrony prywatności w odniesieniu do takich informacji osobowych, obejmujący [wskazanie]: a) gdzie polityka ochrony prywatności jest udostępniona do wglądu publicznego, b) jej dat[ę] obowiązywania, c) biur[a] kontaktowe[go] dla rozpatrywania skarg, wniosków o udzielenie dostępu i wszelkich innych zagadnień wynikających z uczestnictwa w »bezpiecznej przystani«, d) określon[ego] organ[u] ustawow[ego] właściw[ego] do rozpoznawania skarg przeciwko organizacji, dotyczących ewentualnych nieuczciwych lub wprowadzających w błąd praktyk oraz naruszenia przepisów ustawowych lub wykonawczych regulujących ochronę prywatności (wymienion[ego] w załączniku do zasad), e) nazwy wszelkich programów ochrony prywatności, których organizacja jest członkiem, f) metod[y] kontroli (np. wewnętrzna, przez stronę trzecią) […] i g) mechanizm[u] niezależnej ochrony prawnej, który umożliwia badanie nierozstrzygniętych skarg.

W przypadku gdy organizacja chce, aby jej przywileje »bezpiecznej przystani« obejmowały także informacje o zasobach ludzkich, przekazywanych z UE do wykorzystania w związku ze stosunkiem pracy, może tak uczynić w przypadku gdy istnieje ustawowy organ, wymieniony w załączniku do zasad, właściwy do rozpoznawania skarg przeciwko organizacji wynikających z informacji o zasobach ludzkich […].

Departament (albo wyznaczona przez niego osoba) będzie prowadzić wykaz wszystkich organizacji, które złożyły takie pisma, zapewniając sobie w ten sposób przywileje »bezpiecznej przystani« i będzie również aktualizować ten wykaz na podstawie corocznych pism i zawiadomień otrzymanych zgodnie z NZP 11 […].

[…]

NZP 11 – Rozstrzyganie sporów i zapewnianie prawu skuteczności

P: W jaki sposób powinny być wprowadzane w życie wymagania zasady zapewniania prawu skuteczności dotyczące rozstrzygania sporów i jak będzie traktowane uporczywe nieprzestrzeganie zasad przez organizację?

O: Zasada zapewniania prawu skuteczności ustanawia wymagania dotyczące egzekwowania zasad »bezpiecznej przystani«. W NZP dotyczącym kontroli (NZP 7) określono, jak spełnić wymagania [sformułowane w] lit. b) zasad. Niniejsze NZP 11 dotyczy lit. a) i c), które wymagają mechanizmów niezależnej ochrony prawnej. Mechanizmy te mogą przybierać różną postać, ale muszą spełniać wymagania zasady zapewniania prawu skuteczności. Organizacje mogą spełnić te wymagania w następujący sposób: 1) przez przestrzeganie programów ochrony prywatności opracowanych przez sektor prywatny, które włączają zasady »bezpiecznej przystani« do swoich zasad i które zawierają skuteczne mechanizmy zapewniania prawu skuteczności takiego rodzaju jak opisane w zasadzie zapewniania prawu skuteczności; 2) stosując się do wskazówek sądowych i wykonawczych organów nadzorczych, które rozpatrują indywidualne skargi i rozstrzygają spory; lub 3) przez zobowiązanie [się] do współpracy z organami ochrony danych zlokalizowanymi na terytorium Unii Europejskiej lub ich upoważnionymi przedstawicielami. Wykaz ten ma charakter informacyjny, a nie ograniczający. Sektor prywatny może opracować inne mechanizmy zapewniające prawu skuteczność, o ile tylko spełniać one będą wymagania zasady zapewniania prawu skuteczności i NZP. Proszę zauważyć, że wymagania zasady zapewniania prawu skuteczności mają charakter uzupełniający wobec wymagań ustalonych w ust. 3 wstępu do zasad mówiących, że działania samoregulacyjne muszą być egzekwowalne na mocy art. 5 [amerykańskiej] ustawy o Federalnej Komisji Handlu albo podobnej ustawy.

Mechanizmy ochrony prawnej

Powinno się zachęcać konsumentów do składania wszelkich skarg najpierw odnośnym organizacjom, zanim odwołają się do mechanizmów niezależnej ochrony prawnej […].

[…]

Działanie Federalnej Komisji Handlu

FKH (Federalna Komisja Handlu) podjęła się rozpatrywania na zasadzie pierwszeństwa wniosków wpływających od instytucji samoregulujących ochronę prywatności, takich jak BBBOnline i TRUSTe, oraz państw członkowskich podnoszących zarzuty nieprzestrzegania zasad »bezpiecznej przystani« w celu ustalenia, czy zostały naruszone przepisy sekcji 5 [amerykańskiej] ustawy o FKH zakazujące nieuczciwych bądź wprowadzających w błąd czynów lub praktyk handlowych […]”.

10 Zgodnie z załącznikiem IV do decyzji 2000/520:

„Odszkodowania z tytułu naruszenia prywatności, prawne upoważnienia oraz łączenia i przejęcia przedsiębiorstw w prawie amerykańskim

Niniejszy załącznik jest odpowiedzią na zgłoszony przez Komisję Europejską wniosek objaśnienia amerykańskiego prawa dotyczącego a) roszczeń odszkodowawczych z tytułu naruszenia prywatności, b) »wyraźnych upoważnień« w prawie amerykańskim do wykorzystania informacji osobowej w sposób niezgodny z zasadami »bezpiecznej przystani«, i c) łączenia się i przejęć przedsiębiorstw wpływających na zobowiązania podjęte zgodnie z zasadami »bezpiecznej przystani«.

[…]

B. Wyraźne upoważnienia prawne

Zasady »bezpiecznej przystani« zawierają wyjątek w przypadku, gdy przepisy prawa stanowionego albo precedensy stwarzają [ustanawiają] »sprzeczne obowiązki albo wyraźne upoważnienia, pod warunkiem że stosując każde takie upoważnienie, organizacja może wykazać, że nieprzestrzeganie przez nią zasad ogranicza się jedynie do poziomu koniecznego do zaspokojenia nadrzędnych, uzasadnionych interesów popartych takim upoważnieniem«. Najwyraźniej w przypadkach, gdy prawo amerykańskie nakłada sprzeczny obowiązek na organizacje amerykańskie, czy to działające w ramach »bezpiecznej przystani« czy poza nią, muszą one przestrzegać tego prawa. Jeżeli chodzi o wyraźne upoważnienia, podczas, gdy celem zasad »bezpiecznej przystani« jest zatarcie różnic między amerykańskimi a europejskimi systemami ochrony prywatności, ustawodawczym prerogatywom naszych wybranych ustawodawców należne jest poważanie. Ograniczony wyjątek od ścisłego przestrzegania zasad »bezpiecznej przystani« stanowi próbę zachowania równowagi w celu pogodzenia uzasadnionych interesów każdej ze stron.

Wyjątek jest ograniczony do przypadków, w których istnieje wyraźne upoważnienie. Zatem, jako kryterium kwalifikujące, odnośne przepisy prawa stanowionego albo orzeczenie sądowe muszą upoważniać organizację »bezpiecznej przystani« do określonego postępowania […]. Innymi słowy, wyjątku nie stosuje się tam, gdzie prawo tego nie reguluje. Ponadto wyjątek będzie stosowany tylko wtedy, gdy wyraźne upoważnienie jest sprzeczne z przestrzeganiem zasad »bezpiecznej przystani«. Nawet wówczas wyjątek »jest ograniczony do zakresu koniecznego do zaspokojenia nadrzędnych, uzasadnionych interesów popartych takim upoważnieniem«. Dla przykładu, w przypadku gdy prawo po prostu upoważnia przedsiębiorstwo do przekazywania informacji osobowych organom rządowym, wyjątek nie ma zastosowania. I odwrotnie, w przypadku gdy prawo wyraźnie upoważnia przedsiębiorstwo do przekazywania informacji osobowych organom rządowym bez zgody osoby fizycznej, stanowiłoby to »wyraźne upoważnienie« do działania w sposób sprzeczny z zasadami »bezpiecznej przystani«. Alternatywnie, szczególne wyjątki od wymogów dotyczących [ogłoszenia] i zgody wchodziłyby w zakres wyjątku (ponieważ byłoby to równoważne z wyraźnym upoważnieniem do ujawnienia informacji bez ogłoszenia i zgody). Na przykład ustawa, która upoważnia lekarzy do przekazywania dokumentacji medycznej ich pacjentów urzędnikom służby zdrowia bez uprzedniej zgody pacjenta, może dopuszczać wyjątek od zasad ogłoszenia i wyboru. To upoważnienie nie zezwalałoby lekarzowi na udostępnienie tej samej dokumentacji medycznej zakładom opieki zdrowotnej lub komercyjnym farmaceutycznym laboratoriom badawczym, co wykraczałoby poza zakres celów upoważnionych z mocy prawa, a tym samym poza zakres wyjątku […]. Omawiane upoważnienie prawne może być »autonomicznym« upoważnieniem do wykonywania konkretnych czynności z informacjami osobowymi, ale jak pokazują podane niżej przykłady, należy się spodziewać, że będzie to wyjątek od prawa o szerszym zakresie, które zakazuje zbierania, wykorzystywania lub ujawniania informacji osobowych.

[…]”.

Komunikat Komisji COM(2013) 846 final

11 W dniu 27 listopada 2013 r. Komisja przyjęła komunikat do Parlamentu Europejskiego i Rady zatytułowany „Odbudowa zaufania do przepływów danych między Unią Europejską a Stanami Zjednoczonymi” [COM(2013) 846 final, zwany dalej „komunikatem COM(2013) 846 final”]. Komunikatowi temu towarzyszyło sprawozdanie, również z dnia

27 listopada 2013 r., zawierające „ustalenia dokonane przez współprzewodniczących z ramienia Unii w grupie roboczej ad hoc UE–USA ds. ochrony danych” („Report on the Findings by the EU Co-chairs of the ad hoc EU–US Working Group on Data Protection”). Sprawozdanie to zostało przygotowane, jak wskazano w jego pkt 1, we współpracy ze Stanami Zjednoczonymi po ujawnieniu istnienia w tym państwie szeregu programów nadzoru obejmujących gromadzenie i przetwarzanie danych osobowych na znaczną skalę. Sprawozdanie to zawierało między innymi szczegółową analizę porządku prawnego Stanów Zjednoczonych w odniesieniu w szczególności do podstaw prawnych umożliwiających istnienie programów nadzoru, a także gromadzenia i przetwarzania danych osobowych przez amerykańskie władze.

12 W pkt 1 komunikatu COM(2013) 846 final Komisja wyjaśniła, że „[w]ymiana danych do celów komercyjnych została uregulowana w decyzji [2000/520]”, dodając, iż „[d]ecyzja ta stanowi podstawę prawną transferów danych osobowych z UE do przedsiębiorstw mających siedzibę w Stanach Zjednoczonych, które zobowiązały się do przestrzegania zasad bezpiecznego transferu danych osobowych”. Ponadto w tym samym pkt 1 Komisja podkreśliła rosnące znaczenie przepływów danych osobowych, związane w szczególności z rozwojem gospodarki cyfrowej, który „doprowadził do gwałtownego wzrostu ilości, jakości, różnorodności i charakteru działań związanych z przetwarzaniem danych”.

13 W pkt 2 tego komunikatu Komisja zauważyła, że „[w]zrosły jednak obawy co do poziomu ochrony danych osobowych obywateli U[nii] przekazywanych do Stanów Zjednoczonych w ramach […] programu [»Bezpieczna przystań«]”, oraz że „[z]e względu na dobrowolny i deklaratywny charakter systemu wzrosło zainteresowanie jego przejrzystością i kwestią egzekwowania prawa”.

14 Wskazała ona także w tym samym pkt 2, że „[a]merykańskie organy mają dostęp do danych osobowych obywateli Unii przesłanych do Stanów Zjednoczonych w ramach programu »Bezpieczna przystań« i mogą je przetwarzać w sposób niezgodny z powodami, dla których dane te zostały pierwotnie zgromadzone w U[nii], i niezgodny z celem, dla którego zostały one przekazane Stanom Zjednoczonym”, oraz że „[w]iększość amerykańskich przedsiębiorstw internetowych, których [te] programy [nadzoru] prawdopodobnie dotyczą w bardziej bezpośredni sposób, posiada[…] poświadczenia zgodności w ramach programu »Bezpieczna przystań«”.

15 W pkt 3.2 komunikatu COM(2013) 846 final Komisja wskazała na szereg uchybień we wdrażaniu decyzji 2000/520. Stwierdziła ona w tym punkcie z jednej strony, że certyfikowane przedsiębiorstwa amerykańskie nie przestrzegają zasad przewidzianych w art. 1 ust. 1 decyzji 2000/520 (zwanych dalej „zasadami bezpiecznej przystani/bezpiecznego transferu danych”) oraz że wobec tej decyzji należy podjąć działania naprawcze, które powinny dotyczyć „braków strukturalnych związanych z przejrzystością i egzekwowaniem prawa, jak i konkretnych zasad bezpiecznego transferu danych osobowych i funkcjonowania klauzuli bezpieczeństwa narodowego”. Zauważyła ona z drugiej strony, że „[p]rogram »Bezpieczna przystań« działa również jako kanał do przekazywania danych osobowych obywateli Unii z Unii Europejskiej do Stanów Zjednoczonych za pośrednictwem przedsiębiorstw zobowiązanych do przekazania danych amerykańskim służbom wywiadowczym w ramach amerykańskich programów gromadzenia danych”.

16 Komisja uznała w tym pkt 3.2, że jakkolwiek „[z] uwagi na zidentyfikowane uchybienia nie można kontynuować wdrażania decyzji w sprawie ochrony prywatności

w ramach »Bezpiecznej przystani« w obecnej formie [to jednak] [u]chylenie decyzji wpłynęłoby […] negatywnie na interesy przedsiębiorstw członkowskich w Unii Europejskiej i Stanach Zjednoczonych". Komisja dodała w tym samym punkcie, że zamierza „współpracować z amerykańskimi władzami w trybie pilnym w celu omówienia zidentyfikowanych braków".

Komunikat Komisji COM(2013) 847 final

17 W tym samym dniu 27 listopada 2013 r. Komisja przyjęła komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie funkcjonowania zasad bezpiecznego transferu danych osobowych z punktu widzenia obywateli UE i przedsiębiorstw z siedzibą w UE [COM(2013) 847 final, zwany dalej „komunikatem COM(2013) 847 final"]. Jak wynika z pkt 1 tego komunikatu, opiera się on w szczególności na informacjach uzyskanych w ramach grupy kontaktowej [roboczej] UE–USA ad hoc i jest wynikiem dwóch sprawozdań z oceny Komisji opublikowanych, odpowiednio, w 2002 r. i w 2004 r.

18 W pkt 1 tego komunikatu wyjaśniono, że funkcjonowanie decyzji 2000/520 „opiera się na zobowiązaniach i poświadczeniu zgodności uczestniczących przedsiębiorstw", oraz dodano, iż „[z]obowiązanie się do przestrzegania przedmiotowych ustaleń jest dobrowolne, jednak zasady są wiążące dla tych, którzy takie zobowiązanie podejmują".

19 Ponadto z pkt 2.2 komunikatu COM(2013) 847 final wynika, że w dniu 26 września 2013 r. certyfikowanych było 3246 przedsiębiorstw pochodzących z licznych sektorów gospodarki i usług. Przedsiębiorstwa te świadczyły głównie usługi na rynku wewnętrznym Unii, w szczególności w sektorze Internetu, a część z nich to przedsiębiorstwa unijne posiadające spółki zależne w Stanach Zjednoczonych. Część tych przedsiębiorstw przetwarzała dane swoich pracowników z Europy przeniesionych do tego państwa ze względów związanych z organizacją zasobów ludzkich.

20 W tym samym pkt 2.2 Komisja podkreśliła, że „[k]ażda luka w przejrzystości lub egzekwowaniu po stronie Stanów Zjednoczonych powod[owała] przeniesienie odpowiedzialności na europejskie organy ochrony danych i przedsiębiorstwa korzystające z programu".

21 W szczególności z pkt 3–5 i 8 komunikatu COM(2013) 847 final wynika, że w praktyce znaczna liczba przedsiębiorstw nie przestrzegała lub nie w pełni przestrzegała zasad bezpiecznego transferu danych osobowych.

22 Ponadto w pkt 7 tego samego komunikatu Komisja wskazała, że „wszystkie przedsiębiorstwa, które biorą udział w programie PRISM [programie gromadzenia informacji na znaczną skalę] i udzielają dostępu organom Stanów Zjednoczonych do danych przechowywanych i przetwarzanych w Stanach Zjednoczonych, dokonały poświadczenia zgodności z programem bezpiecznego transferu danych" oraz że w ten sposób stał się on „jednym z kanałów dostępu organów wywiadowczych Stanów Zjednoczonych do danych osobowych wstępnie przetworzonych w U[nii]". W tym względzie Komisja stwierdziła w pkt 7.1 rzeczonego komunikatu, że „w szeregu podstaw prawnych w prawie Stanów Zjednoczonych dopuszcza się gromadzenie i przetwarzanie na szeroką skalę danych osobowych przechowywanych lub w inny sposób przetwarzanych przez przedsiębiorstwa z siedzibą w Stanach Zjednoczonych" oraz że „[s]zeroko zakrojony charakter takich programów może prowadzić do uzyskiwania dostępu i dalszego przetwarzania przez organy

Stanów Zjednoczonych danych przekazywanych w ramach programu bezpiecznego transferu danych w stopniu wykraczającym poza zakres ściśle niezbędny i proporcjonalny do ochrony bezpieczeństwa narodowego, przewidziany w wyjątku określonym w decyzji w sprawie bezpiecznego transferu danych osobowych".

23 W pkt 7.2 komunikatu COM(2013) 847 final, zatytułowanym „Ograniczenia i możliwości dochodzenia roszczeń", Komisja podkreśliła, że „gwarancje przewidziane w prawie Stanów Zjednoczonych są głównie dostępne dla obywateli lub legalnych rezydentów Stanów Zjednoczonych" oraz że „[p]onadto ani w U[nii] ani w Stanach Zjednoczonych osoby, których dane dotyczą, nie mają możliwości uzyskania dostępu do danych, ich zmiany ani usunięcia. Nie istnieją również środki odwoławcze na drodze sądowej lub administracyjnej w związku z gromadzeniem i dalszym przetwarzaniem danych osobowych takich osób w ramach amerykańskich programów nadzoru".

24 Zgodnie z pkt 8 komunikatu COM(2013) 847 final wśród certyfikowanych przedsiębiorstw znajdują się „[p]rzedsiębiorstwa internetowe, takie jak Google, Facebook, Microsoft, Apple, Yahoo", posiadające „setki milionów klientów w Europie" i przekazujące dane osobowe w celu ich przetwarzania do Stanów Zjednoczonych.

25 Komisja uznała w tym samym pkt 8, że „szeroki dostęp agencji wywiadowczych do danych przekazywanych Stanom Zjednoczonym przez przedsiębiorstwa, które dokonały poświadczenia zgodności z zasadami bezpiecznego transferu danych osobowych, budzi dodatkowe poważne wątpliwości co do ciągłości przestrzegania praw Europejczyków do ochrony danych w przypadku przekazywania ich danych Stanom Zjednoczonym".

Postępowanie główne i pytania prejudycjalne

26 Maximillian Schrems, obywatel austriacki mieszkający w Austrii, jest użytkownikiem sieci społecznościowej Facebook (zwanej dalej „Facebookiem") od 2008 r.

27 Od wszystkich osób mieszkających na terytorium Unii i chcących używać Facebooka wymagane jest zawarcie, w chwili rejestracji, umowy ze spółką Facebook Ireland, będącą spółką zależną spółki dominującej Facebook Inc., mającej siedzibę w Stanach Zjednoczonych. Dane osobowe użytkowników Facebooka mieszkających na terytorium Unii są, w całości lub częściowo, przekazywane na serwery spółki Facebook Inc., położone na terytorium Stanów Zjednoczonych, gdzie dane te są przetwarzane.

28 W dniu 25 czerwca 2013 r. M. Schrems złożył skargę do komisarza, w której zażądał w istocie, aby organ ten, w wykonaniu swoich kompetencji, zakazał spółce Facebook Ireland przekazywania jego danych osobowych do Stanów Zjednoczonych. Maximilian Schrems podniósł w tej skardze, że prawo i praktyka obowiązujące we wskazanym państwie nie zapewniają wystarczającej ochrony danych osobowych przechowywanych na jego terytorium przed działaniami nadzorczymi prowadzonymi w nim przez władze publiczne. Maximillian Schrems odniósł się w tym względzie do informacji ujawnionych przez E. Snowdena na temat działalności amerykańskich służb wywiadowczych, a w szczególności służb National Security Agency (zwanej dalej „NSA").

29 Komisarz uznał, że nie miał obowiązku przeprowadzenia dochodzenia w przedmiocie okoliczności faktycznych wskazanych przez M. Schremsa w skardze i odrzucił tę skargę jako bezpodstawną. Uznał bowiem, że nie ma dowodów na to, iż NSA uzyskała dostęp do danych

osobowych zainteresowanego. Komisarz dodał, że zarzuty podniesione przez M. Schremsa w jego skardze nie mogą być skuteczne, ponieważ wszelkie kwestie dotyczące odpowiedniości stopnia ochrony tych danych w Stanach Zjednoczonych należy rozpatrywać zgodnie z decyzją 2000/520, zaś w decyzji tej Komisja stwierdziła, że Stany Zjednoczone zapewniały odpowiedni stopień ochrony.

30 Maximillian Schrems wniósł na decyzję sporną w postępowaniu głównym skargę do High Court (sądu najwyższego). Po zbadaniu dowodów przedstawionych przez strony w postępowaniu głównym sąd ten stwierdził, że nadzór elektroniczny i przechwytywanie danych osobowych przekazywanych z Unii do Stanów Zjednoczonych służyło realizacji koniecznych i niezbędnych celów interesu publicznego. Sąd ten dodał jednak, że informacje ujawnione przez E. Snowdena wskazały na „istotne przekroczenie granic kompetencji" ze strony NSA i innych organów federalnych.

31 Zdaniem tego samego sądu obywatele Unii nie mają zagwarantowanego skutecznego prawa do bycia wysłuchanym. Nadzór nad działaniami służb wywiadowczych sprawowany jest w ramach tajnej i niekontradyktoryjnej procedury. Po przekazaniu danych osobowych do Stanów Zjednoczonych NSA, a także inne agencje federalne, takie jak Federal Bureau of Investigation (FBI), mogą uzyskać do nich dostęp w ramach dokonywanego przez siebie niezróżnicowanego nadzoru oraz przechwytywania, prowadzonych przez te agencje na znaczną skalę.

32 High Court stwierdził, że prawo irlandzkie zakazuje przekazywania danych osobowych poza terytorium krajowe, z wyjątkiem przypadków, w których dane państwo trzecie zapewnia odpowiedni stopień ochrony życia prywatnego oraz praw i wolności podstawowych. Znaczenie praw do życia prywatnego i nienaruszalności mieszkania, gwarantowanych w irlandzkiej konstytucji, wymaga, aby wszelka ingerencja w te prawa była proporcjonalna i zgodna z wymogami przewidzianymi w ustawie.

33 Masowy i niezróżnicowany dostęp do danych osobowych jest w oczywisty sposób sprzeczny z zasadą proporcjonalności i podstawowymi wartościami chronionymi przez irlandzką konstytucję. Dla uznania przechwytywania wiadomości elektronicznych za zgodne z tą konstytucją należy przedstawić dowody na to, że takie przechwytywanie ma charakter indywidualny, że nadzór określonych osób lub określonych grup jest uzasadniony na podstawie obiektywnych przesłanek w interesie zapewniania bezpieczeństwa narodowego lub zwalczania przestępczości oraz że istnieją odpowiednie i możliwe do zweryfikowania gwarancje. Zatem zdaniem High Court gdyby sprawa w postępowaniu głównym miała zostać rozstrzygnięta wyłącznie na podstawie prawa irlandzkiego, należałoby stwierdzić – uwzględniając poważne wątpliwości co do tego, czy Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych – że komisarz miał obowiązek przeprowadzenia dochodzenia w przedmiocie okoliczności faktycznych przedstawionych przez M. Schremsa w jego skardze, którą komisarz niesłusznie oddalił.

34 W każdym razie High Court stwierdził, że niniejsza sprawa dotyczy stosowania prawa Unii w rozumieniu art. 51 karty, a więc zgodność z prawem decyzji spornej w postępowaniu głównym należy oceniać z punktu widzenia prawa Unii. Zdaniem tego sądu decyzja 2000/520 nie spełnia wymogów wynikających z art. 7 i 8 karty ani zasad sformułowanych przez Trybunał w wyroku Digital Rights Ireland i in. (C-293/12 i C-594/12, EU:C:2014:238). Prawo do poszanowania życia prywatnego, gwarantowane przez art. 7 karty oraz przez istotne wartości wspólne dla tradycji państw członkowskich, zostałoby pozbawione znaczenia, gdyby

organy publiczne mogły uzyskać dowolny i powszechny dostęp do wiadomości elektronicznych bez obiektywnego uzasadnienia opartego na względach bezpieczeństwa narodowego lub zapobiegania przestępczości związanych w szczególny sposób z zainteresowanymi jednostkami i bez otoczenia tych praktyk odpowiednimi i wiarygodnymi gwarancjami.

35 High Court zauważył ponadto, że M. Schrems w rzeczywistości podważa w swojej skardze zgodność z prawem systemu „bezpiecznej przystani" wprowadzonego w życie decyzją 2000/520, z którego wynika decyzja sporna w postępowaniu głównym. Jakkolwiek M. Schrems nie podważa formalnie ważności ani dyrektywy 95/46, ani decyzji 2000/520, to jednak zdaniem tego sądu powstaje pytanie, czy na mocy art. 25 ust. 6 dyrektywy 95/46 komisarz był związany ustaleniami dokonanymi przez Komisję w decyzji 2000/520, zgodnie z którymi Stany Zjednoczone zapewniają odpowiedni stopień ochrony, czy też art. 8 karty upoważnia komisarza do odstąpienia, w razie potrzeby, od tych ustaleń.

36 W tych okolicznościach High Court postanowił zawiesić postępowanie i przedłożyć Trybunałowi następujące pytania prejudycjalne:

„1) Czy jeżeli w trakcie rozpatrywania skargi skierowanej do niezależnego urzędnika, któremu z mocy ustawy powierzono funkcje administracyjne i wykonawcze w odniesieniu do ustawodawstwa dotyczącego ochrony danych, dane osobowe przekazywane są do innego państwa trzeciego (w tym przypadku do Stanów Zjednoczonych Ameryki), którego obowiązujące przepisy i praktyka prawna nie gwarantują w ocenie skarżącego adekwatnej [odpowiedniego stopnia] ochrony osoby, której owe dane dotyczą, urzędnik ten jest – uwzględniając art. 7, 8 i 47 karty i niezależnie od [bez uszczerbku dla] przepisu art. 25 ust. 6 dyrektywy 95/46 – bezwzględnie związany odmiennymi ustaleniami Unii zawartymi w decyzji Komisji 2000/520?

2) Ewentualnie, czy urzędnik ten może, czy też musi zbadać tę sprawę indywidualnie w świetle nowych okoliczności faktycznych zaistniałych w międzyczasie, po dacie publikacji decyzji Komisji?".

W przedmiocie pytań prejudycjalnych

37 W swoich pytaniach prejudycjalnych, które należy zbadać łącznie, sąd odsyłający zmierza w istocie do ustalenia, czy – i w jakim stopniu – art. 25 ust. 6 dyrektywy 95/46 w związku z art. 7, 8 i 47 karty należy interpretować w ten sposób, że decyzja przyjęta na podstawie tego przepisu, taka jak decyzja 2000/520, w której Komisja stwierdza, że państwo trzecie zapewnia odpowiedni stopień ochrony, stoi na przeszkodzie temu, aby organ nadzorczy państwa członkowskiego, w rozumieniu art. 28 tej dyrektywy, mógł rozpatrzyć skargę osoby dotyczącą ochrony jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, które zostały przekazane z państwa członkowskiego do państwa trzeciego, podczas gdy osoba ta podnosi, że obowiązujące w tym państwie trzecim prawo i praktyki nie zapewniają odpowiedniego stopnia ochrony.

W przedmiocie kompetencji krajowych organów nadzorczych w rozumieniu art. 28 dyrektywy 95/46 w świetle decyzji Komisji przyjętej na podstawie art. 25 ust. 6 tej dyrektywy

38 Na wstępie należy przypomnieć, że przepisy dyrektywy 95/46 regulujące kwestię przetwarzania danych osobowych mogącego naruszyć podstawowe wolności,

a w szczególności prawo do poszanowania życia prywatnego, muszą być bezwzględnie interpretowane z punktu widzenia praw podstawowych gwarantowanych w karcie (zob. wyroki: Österreichischer Rundfunk i in., C-465/00, C-138/01 i C-139/01, EU:C:2003:294, pkt 68; Google Spain i Google, C-131/12, EU:C:2014:317, pkt 68; a także Ryneš, C-212/13, EU:C:2014:2428, pkt 29).

39 Z art. 1, a także motywów 2 i 10 dyrektywy 95/46 wynika, że jej celem jest nie tylko zapewnienie skutecznej i pełnej ochrony podstawowych praw i wolności osób fizycznych, a szczególnie prawa podstawowego do poszanowania prywatności w zakresie przetwarzania danych osobowych, ale również wysokiego poziomu ochrony tych podstawowych praw i wolności. Znaczenie zarówno prawa podstawowego do poszanowania życia prywatnego, gwarantowanego w art. 7 karty, jak i prawa podstawowego do ochrony danych osobowych, gwarantowanego w jej art. 8, zostało ponadto podkreślone w orzecznictwie Trybunału (zob. wyroki: Rijkeboer, C-553/07, EU:C:2009:293, pkt 47; Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 53; a także Google Spain i Google, C-131/12, EU:C:2014:317, pkt 53, 66, 74 i przytoczone tam orzecznictwo).

40 Jeśli chodzi o kompetencje przysługujące krajowym organom nadzorczym w odniesieniu do przekazywania danych osobowych do państw trzecich, należy wskazać, że art. 28 ust. 1 akapit drugi dyrektywy 95/46 nakłada na państwa członkowskie obowiązek utworzenia jednego lub większej liczby organów nadzorujących, w sposób całkowicie niezależny, poszanowanie unijnych zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania takich danych. Wymóg ten wynika również z pierwotnego prawa Unii, a w szczególności z art. 8 ust. 3 karty i z art. 16 ust. 2 TFUE (zob. podobnie wyroki: Komisja/Austria, C-614/10, EU:C:2012:631, pkt 36; a także Komisja/Węgry, C-288/12, EU:C:2014:237, pkt 47).

41 Zagwarantowanie niezależności krajowych organów nadzorczych ma na celu zapewnienie skuteczności i pewności kontroli przestrzegania przepisów w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i powinno być interpretowane w świetle tego celu. Ta gwarancja niezależności została wprowadzona dla wzmocnienia ochrony osób i instytucji, których dotyczą decyzje tych organów. Ustanowienie w państwach członkowskich niezależnych organów nadzorczych stanowi zatem, jak wskazuje motyw 62 dyrektywy 95/46, istotny element ochrony osób w związku z przetwarzaniem danych osobowych (zob. wyroki: Komisja/Niemcy, C-518/07, EU:C:2010:125, pkt 25; a także Komisja/Węgry C-288/12, EU:C:2014:237, pkt 48 i przytoczone tam orzecznictwo).

42 Celem zagwarantowania takiej ochrony krajowe organy nadzorcze powinny w szczególności zapewnić prawidłową równowagę pomiędzy z jednej strony przestrzeganiem podstawowego prawa do poszanowania życia prywatnego a z drugiej strony interesami, które wymagają swobodnego przepływu danych osobowych (zob. podobnie wyroki: Komisja/Niemcy, C-518/07, EU:C:2010:125, pkt 24; Komisja/Węgry, C-288/12, EU:C:2014:237, pkt 51).

43 Jak podkreślono w motywie 63 dyrektywy 95/46, organy te dysponują w tym celu szerokim wachlarzem kompetencji, które, wymienione w sposób niewyczerpujący w art. 28 ust. 3 owej dyrektywy, stanowią środki niezbędne do wykonywania ich zadań. Organom tym przysługują zatem kompetencje dochodzeniowe, takie jak prawo do gromadzenia wszelkich informacji potrzebnych do wykonywania ich funkcji nadzorczych, skuteczne kompetencje

interwencyjne, takie jak prawo nakładania czasowego lub ostatecznego zakazu przetwarzania danych oraz prawo pozywania.

44 Co prawda z art. 28 ust. 1 i 6 dyrektywy 95/46 wynika, że kompetencje krajowych organów nadzorczych dotyczą przetwarzania danych osobowych dokonywanego na terytorium państwa członkowskiego, do którego te organy należą, a więc nie posiadają one na mocy tego art. 28 kompetencji w odniesieniu do przetwarzania tychże danych dokonywanego na terytorium państwa trzeciego.

45 Jednak operacja przekazywania danych osobowych z państwa członkowskiego do państwa trzeciego polega sama w sobie na przetwarzaniu danych osobowych w rozumieniu art. 2 lit. b) dyrektywy 95/46 (zob. podobnie wyrok Parlament/Rada i Komisja, C-317/04 i C-318/04, EU:C:2006:346, pkt 56) dokonywanym na terytorium państwa członkowskiego. Przepis ten definiuje bowiem „przetwarzanie danych osobowych" jako „każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych" i wskazuje jako przykład „ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób".

46 W motywie 60 dyrektywy 95/46 wyjaśniono, że przekazywanie danych osobowych do państw trzecich może następować jedynie w pełnej zgodności z przepisami przyjętymi przez państwa członkowskie na podstawie tej dyrektywy. W tym względzie rozdział IV omawianej dyrektywy, w którym zawarte są jej art. 25 i 26, ustanowił system służący zapewnieniu przez państwa członkowskie kontroli nad przekazywaniem danych osobowych do państw trzecich. System ten stanowi uzupełnienie ogólnego systemu wprowadzonego w rozdziale II tej dyrektywy, przewidującym ogólne kryteria legalności przetwarzania danych osobowych (zob. podobnie wyrok Lindqvist, C-101/01, EU:C:2003:596, pkt 63).

47 Skoro krajowe organy nadzorcze, zgodnie z art. 8 ust. 3 karty i z art. 28 dyrektywy 95/46, zobowiązane są kontrolować poszanowanie unijnych zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych, każdy z nich jest więc wyposażony w kompetencję do zbadania, czy przekazywanie danych osobowych z państwa członkowskiego, do którego on należy, do państwa trzeciego następuje z poszanowaniem wymogów formułowanych przez dyrektywę 95/46.

48 Uznając w swoim motywie 56, że przekazywanie danych osobowych z państw członkowskich do państw trzecich jest koniecznym warunkiem rozwoju handlu międzynarodowego, w art. 25 ust. 1 dyrektywa 95/46 ustanawia zasadę, zgodnie z którą takie przekazywanie może następować wyłącznie w sytuacji, gdy to państwo trzecie zapewnia odpowiedni stopień ochrony.

49 Ponadto w motywie 57 omawianej dyrektywy wyjaśniono, że należy zakazać przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony.

50 W celu dokonywania kontroli przekazywania danych osobowych do państw trzecich – w zależności od poziomu ochrony zapewnianego danym osobowym w każdym z tych państw – art. 25 dyrektywy 95/46 nakłada na państwa członkowskie i Komisję szereg obowiązków. Z przepisu tego wynika w szczególności, że ustalenia dotyczące tego, czy państwo trzecie zapewnia odpowiedni stopień ochrony, czy też nie, mogą zostać, jak wskazał rzecznik generalny w pkt 86 opinii, dokonane albo przez państwa członkowskie, albo przez Komisję.

51 Komisja może przyjąć na podstawie art. 25 ust. 6 dyrektywy 95/46 decyzję stwierdzającą, że państwo trzecie zapewnia odpowiedni stopień ochrony. Decyzja taka skierowana jest, zgodnie z akapitem drugim tego przepisu, do państw członkowskich, które podejmują środki niezbędne w celu jej wykonania. Zgodnie z art. 288 akapit czwarty TFUE wiąże ona wszystkie państwa członkowskie, do których jest skierowana, a w związku z tym jest wiążąca dla wszystkich ich organów (zob. podobnie wyroki: Albako Margarinefabrik, 249/85, EU:C:1987:245, pkt 17; Mediaset, C-69/13, EU:C:2014:71, pkt 23) w zakresie, w jakim skutkuje ona upoważnieniem do przekazywania danych osobowych z państw członkowskich do wskazanych w niej państw trzecich.

52 Dopóki zatem Trybunał nie stwierdzi nieważności decyzji Komisji, dopóty państwa członkowskie i ich organy, w tym ich niezależne organy nadzorcze, nie mogą co prawda przyjmować środków sprzecznych z tą decyzją, takich jak akty zmierzające do stwierdzenia w sposób wiążący, że państwo trzecie, którego dotyczy omawiana decyzja, nie zapewnia odpowiedniego stopnia ochrony. Akty instytucji Unii korzystają bowiem zasadniczo z domniemania ważności, a zatem wywołują skutki prawne do czasu ich uchylenia, stwierdzenia ich nieważności w ramach skargi o stwierdzenie nieważności lub uznania ich za nieważne w następstwie wniosku o wydanie orzeczenia w trybie prejudycjalnym lub zarzutu niezgodności z prawem (wyrok Komisja/Grecja, C-475/01, EU:C:2004:585, pkt 18 i przytoczone tam orzecznictwo).

53 Jednak decyzja Komisji przyjęta zgodnie z art. 25 ust. 6 dyrektywy 95/46, taka jak decyzja 2000/520, nie uniemożliwia osobom, których dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego, wniesienia do krajowych organów nadzorczych skargi w rozumieniu art. 28 ust. 4 tej dyrektywy, dotyczącej ochrony ich praw i wolności w odniesieniu do przetwarzania tych danych. Co więcej, taka decyzja, jak wskazał rzecznik generalny w szczególności w pkt 61, 93 i 116 opinii, nie może zanegować ani ograniczyć kompetencji wyraźnie przyznanych krajowym organom nadzorczym w art. 8 ust. 3 karty oraz w art. 28 omawianej dyrektywy.

54 Ani art. 8 ust. 3 karty, ani art. 28 dyrektywy 95/46 nie wykluczają z zakresu kompetencji krajowych organów nadzorczych kontroli przekazywania danych osobowych do państw trzecich będących przedmiotem decyzji Komisji przyjętej na mocy art. 25 ust. 6 tej dyrektywy.

55 W szczególności art. 28 ust. 4 akapit pierwszy dyrektywy 95/46, który stanowi, że do krajowych organów nadzorczych może wnieść skargę „dowoln[a] osob[a] […] odnośnie do ochrony jej praw i wolności w zakresie przetwarzania danych osobowych”, nie przewiduje żadnego wyjątku w tym względzie w sytuacji, gdy Komisja przyjęła decyzję na podstawie art. 25 ust. 6 tej dyrektywy.

56 Ponadto sprzeczna z systemem wprowadzonym przez dyrektywę 95/46, a także z celem jej art. 25 i 28 byłaby sytuacja, w której decyzja Komisji przyjęta na podstawie art. 25 ust. 6 omawianej dyrektywy skutkowałaby uniemożliwieniem krajowemu organowi nadzorczemu rozpatrzenia skargi osoby, dotyczącej ochrony jej praw i wolności w zakresie przetwarzania jej danych osobowych, które zostały lub mogły zostać przekazane z państwa członkowskiego do państwa trzeciego, którego dotyczy ta decyzja.

57 Przeciwnie, art. 28 dyrektywy 95/46 ma zastosowanie – z samej swojej natury – do wszelkiego przetwarzania danych osobowych. W ten sposób, nawet jeśli istnieje decyzja

Komisji przyjęta na podstawie art. 25 ust. 6 tej dyrektywy, krajowe organy nadzorcze, do których osoba wniosła skargę dotyczącą ochrony jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, powinny móc zbadać w sposób całkowicie niezależny, czy przekazywanie tych danych nastąpiło z poszanowaniem wymogów formułowanych przez omawianą dyrektywę.

58 Gdyby tak nie było, osoby, których dane osobowe zostały lub mogły zostać przekazane do danego państwa trzeciego, zostałyby pozbawione prawa, gwarantowanego przez art. 8 ust. 1 i 3 karty, do zwrócenia się do krajowych organów nadzorczych ze skargą służącą ochronie ich praw podstawowych (zob. analogicznie wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 68).

59 Skargę w rozumieniu art. 28 ust. 4 dyrektywy 95/46, w której osoba, której dane osobowe zostały lub mogły zostać przekazane do państwa trzeciego, podnosi – jak w postępowaniu głównym – że prawo i praktyki danego państwa trzeciego nie zapewniają, niezależnie od ustaleń Komisji w decyzji przyjętej na podstawie art. 25 ust. 6 tej dyrektywy, odpowiedniego poziomu ochrony, należy rozumieć jako dotyczącą w istocie zgodności tej decyzji z ochroną życia prywatnego oraz wolności i praw podstawowych jednostek.

60 W tym względzie należy przypomnieć utrwalone orzecznictwo Trybunału, zgodnie z którym Unia jest unią prawa, w której akty instytucji podlegają kontroli pod względem zgodności między innymi z traktatami, ogólnymi zasadami prawa oraz prawami podstawowymi (zob. podobnie wyroki: Komisja i in./Kadi, C-584/10 P, C-593/10 P i C-595/10 P, EU:C:2013:518, pkt 66; Inuit Tapiriit Kanatami i in./Parlament i Rada, C-583/11 P, EU:C:2013:625, pkt 91; a także Telefónica/Komisja C-274/12 P, EU:C:2013:852, pkt 56). Decyzje Komisji przyjęte na podstawie art. 25 ust. 6 dyrektywy 95/46 nie mogą być z tej kontroli zwolnione.

61 Jedynie Trybunał jest przy tym właściwy do stwierdzenia, że akt Unii, taki jak decyzja Komisji przyjęta na podstawie art. 25 ust. 6 dyrektywy 95/46, jest nieważny, a celem tej wyłącznej kompetencji jest zapewnienie pewności prawa poprzez jednolite stosowanie prawa Unii (zob. wyroki: Melki i Abdeli, C-188/10 i C-189/10, EU:C:2010:363, pkt 54; a także CIVAD, C-533/10, EU:C:2012:347, pkt 40).

62 O ile sądy krajowe mają co prawda prawo badać ważność aktu unijnego, takiego jak decyzja Komisji przyjęta na podstawie art. 25 ust. 6 dyrektywy 95/46, o tyle jednak nie są one właściwe do samodzielnego stwierdzenia nieważności takiego aktu (zob. wyroki: Foto-Frost, 314/85, EU:C:1987:452, pkt 15–20; a także IATA i ELFAA, C-344/04, EU:C:2006:10, pkt 27). A fortiori, krajowe organy nadzorcze nie mają prawa samodzielnie stwierdzić nieważności takiej decyzji przy rozpatrywaniu skargi, w rozumieniu art. 28 ust. 4 tej dyrektywy, dotyczącej zgodności decyzji Komisji przyjętej na podstawie art. 25 ust. 6 omawianej dyrektywy z ochroną życia prywatnego oraz podstawowych praw i wolności jednostek.

63 Z uwagi na te rozważania, jeśli 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, podobnie jak w postępowaniu głównym, 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.

64 Jeśli omawiany organ dojdzie do wniosku, że zarzuty podniesione na poparcie takiej skargi są bezzasadne, i oddali tę skargę z tego powodu, osobie, która ją wniosła, musi – jak wynika z art. 28 ust. 3 akapit drugi dyrektywy 95/46 w związku z art. 47 karty – przysługiwać prawo odwołania do sądu, umożliwiające jej podważenie tej niekorzystnej dla niej decyzji przed sądami krajowymi. Biorąc pod uwagę orzecznictwo przytoczone w pkt 61 i 62 niniejszego wyroku, owe sądy krajowe zobowiązane są zawiesić postępowanie i zwrócić się do Trybunału z pytaniem prejudycjalnym dotyczącym ważności, jeżeli uznają one za zasadne zarzut lub zarzuty nieważności podniesione przez strony lub ewentualnie uwzględnione z urzędu (zob. podobnie wyrok T & L Sugars i Sidul Açúcares/Komisja, C-456/13 P, EU:C:2015:284, pkt 48 i przytoczone tam orzecznictwo).

65 W przeciwnej sytuacji, w której omawiany organ uzna zarzuty podniesione przez osobę, która wniosła do niego skargę dotyczącą ochrony jej praw i wolności w zakresie przetwarzania danych osobowych, za zasadne, organ ten powinien – zgodnie z art. 28 ust. 3 akapit pierwszy 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.

66 Biorąc pod uwagę powyższe rozważania, na przedstawione pytania prejudycjalne należy odpowiedzieć, że art. 25 ust. 6 dyrektywy 95/46 w związku z art. 7, 8 i 47 karty należy interpretować w ten sposób, iż decyzja przyjęta na podstawie tego przepisu, taka jak decyzja 2000/520, w której Komisja stwierdza, że państwo trzecie zapewnia odpowiedni stopień ochrony, nie stoi na przeszkodzie temu, aby krajowy organ nadzorczy państwa członkowskiego, w rozumieniu art. 28 tej dyrektywy, rozpatrzył skargę danej osoby dotyczącą ochrony jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, które zostały przekazane z państwa członkowskiego do tego państwa trzeciego, kiedy osoba ta podnosi, że obowiązujące w tym państwie trzecim prawo i praktyki nie zapewniają odpowiedniego stopnia ochrony.

W przedmiocie ważności decyzji 2000/520

67 Jak wynika z wyjaśnień sądu odsyłającego dotyczących przedstawionych pytań, M. Schrems podnosi w postępowaniu głównym, że prawo i praktyki Stanów Zjednoczonych nie zapewniają odpowiedniego stopnia ochrony w rozumieniu art. 25 dyrektywy 95/46. Jak wskazał rzecznik generalny w pkt 123 i 124 opinii, M. Schrems wyraża wątpliwości, które sąd odsyłający wydaje się skądinąd podzielać, co do ważności decyzji 2000/520. W tych okolicznościach, z uwzględnieniem ustaleń dokonanych w pkt 60–63 niniejszego wyroku i w celu udzielenia temu sądowi pełnej odpowiedzi, należy zbadać, czy decyzja ta jest zgodna z wymogami wynikającymi z owej dyrektywy w związku z kartą.

W przedmiocie wymogów wynikających z art. 25 ust. 6 dyrektywy 95/46

68 Jak już wskazano w pkt 48 i 49 niniejszego wyroku, art. 25 ust. 1 dyrektywy 95/46 zakazuje przekazywania danych osobowych do państw trzecich, które nie zapewniają odpowiedniego stopnia ochrony.

69 Jednakże dla celów kontroli takiego przekazywania danych osobowych w art. 25 ust. 6 akapit pierwszy tej dyrektywy przewidziano, iż Komisja „może stwierdzić […], że państwo trzecie zapewnia prawidłowy stopień ochrony w znaczeniu ust. 2 [tego artykułu], co wynika z jego prawa krajowego lub międzynarodowych zobowiązań, […] w zakresie ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych”.

70 Co prawda ani art. 25 ust. 2 dyrektywy 95/46, ani żaden inny jej przepis nie zawierają definicji pojęcia „odpowiedniego stopnia ochrony”. W szczególności art. 25 ust. 2 tej dyrektywy ogranicza się do stwierdzenia, że odpowiedni stopień ochrony danych zapewnianej przez państwo trzecie „należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji”, i wymienia w sposób niewyczerpujący okoliczności, jakie należy wziąć pod uwagę przy dokonywaniu takiej oceny.

71 Tym niemniej z jednej strony z samego brzmienia art. 25 ust. 6 dyrektywy 95/46 wynika, że przepis ten wymaga, aby państwo trzecie „zapewniało” odpowiedni poziom ochrony ze względu na swoje wewnętrzne ustawodawstwo i swoje zobowiązania międzynarodowe. Z drugiej strony – również zgodnie z tym przepisem – odpowiedni stopień ochrony zapewnianej przez to państwo trzecie należy oceniać „w zakresie [w odniesieniu do] ochrony życia prywatnego i podstawowych praw i wolności osób fizycznych”.

72 W ten sposób art. 25 ust. 6 dyrektywy 95/46 wprowadza w życie wyraźny obowiązek ochrony danych osobowych, przewidziany w art. 8 ust. 1 karty, i zmierza do zapewnienia, jak wskazał rzecznik generalny w pkt 139 opinii, utrzymania wysokiego poziomu tej ochrony w przypadku przekazywania danych osobowych do państw trzecich.

73 Oczywiście termin „odpowiedni” zawarty w art. 25 ust. 6 dyrektywy 95/46 oznacza, że od państwa trzeciego nie można wymagać zapewnienia poziomu ochrony identycznego z tym, jaki jest zagwarantowany w unijnym porządku prawnym. Tym niemniej, jak wskazał rzecznik generalny w pkt 141 opinii, wyrażenie „odpowiedni stopień ochrony” należy rozumieć jako wymagające od tego państwa trzeciego skutecznego zapewnienia, ze względu na jego ustawodawstwo wewnętrzne lub zobowiązania międzynarodowe, poziomu ochrony podstawowych praw i wolności merytorycznie równoważnego poziomowi gwarantowanemu w Unii na mocy dyrektywy 95/46 w związku z kartą. W braku takiego wymogu cel wymieniony w poprzedzającym punkcie niniejszego wyroku zostałby bowiem zaprzepaszczony. Ponadto wysoki poziom ochrony gwarantowany w dyrektywie 95/46 w związku z kartą można byłoby łatwo obejść poprzez przekazanie danych osobowych z Unii do państw trzecich w celu ich przetwarzania w tych państwach.

74 Z wyraźnego brzmienia art. 25 ust. 6 dyrektywy 95/46 wynika, że to właśnie porządek prawny państwa trzeciego, którego dotyczy decyzja Komisji, powinien zapewniać odpowiedni stopień ochrony. Jakkolwiek środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii w celu zagwarantowania poszanowania wymogów płynących z tej dyrektywy w związku z kartą, to jednak środki te powinny w praktyce skutecznie zapewniać ochronę merytorycznie równoważną ochronie gwarantowanej w Unii.

75 W tych okolicznościach przy badaniu poziomu ochrony zapewnionego w państwie trzecim Komisja zobowiązana jest ocenić treść reguł mających zastosowanie w tym państwie wynikających z jego ustawodawstwa wewnętrznego lub ze zobowiązań międzynarodowych, a także praktykę zmierzającą do zapewnienia poszanowania tych reguł, przy czym instytucja ta powinna zgodnie z art. 25 ust. 2 dyrektywy 95/46 wziąć pod uwagę wszystkie okoliczności dotyczące przekazywania danych osobowych do państwa trzeciego.

76 Co więcej, w związku z tym, że poziom ochrony zapewniony w państwie trzecim może zmieniać się w czasie, do Komisji należy, po przyjęciu decyzji na podstawie art. 25 ust. 6 dyrektywy 95/46, okresowe badanie, czy przy uwzględnieniu stanu faktycznego i prawnego ustalenia poczynione co do odpowiedniego stopnia ochrony zapewnionego przez dane państwo trzecie są nadal zasadne. Takie badanie należy przeprowadzić w każdym razie wówczas, gdy wyjdą na jaw okoliczności mogące wzbudzić co do tego wątpliwości.

77 W każdym razie, jak wskazał rzecznik generalny w pkt 134 i 135 opinii, przy badaniu ważności decyzji Komisji przyjętej na mocy art. 25 ust. 6 dyrektywy 95/46 należy również uwzględnić okoliczności występujące po przyjęciu tej decyzji.

78 Należy w tym względzie stwierdzić, że mając na uwadze, po pierwsze, znaczącą rolę, jaką odgrywa ochrona danych osobowych w świetle prawa podstawowego do poszanowania życia prywatnego, oraz po drugie, znaczną liczbę osób, których prawa podstawowe mogą zostać naruszone w przypadku przekazania danych osobowych do państwa trzeciego niezapewniającego odpowiedniego stopnia ochrony, kompetencje ocenne Komisji w odniesieniu do odpowiedniego poziomu ochrony zapewnionego w państwie trzecim są ograniczone, skutkiem czego kontrola wymogów wynikających z art. 25 dyrektywy 95/46 w związku z kartą musi mieć charakter ścisły (zob. analogicznie wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 47, 48).

W przedmiocie art. 1 decyzji 2000/520

79 Komisja uznała w art. 1 ust. 1 decyzji 2000/520, że zasady określone w załączniku I do decyzji 2000/520, wprowadzane w życie zgodnie z wytycznymi dostarczonymi przez NZP zawarte w załączniku II do tej decyzji, zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z Unii do organizacji mających siedzibę w Stanach Zjednoczonych. Z przepisu tego wynika, że zarówno te zasady, jak i te NZP zostały opublikowane przez Departament Handlu USA.

80 Jak wynika z art. 1 ust. 2 i 3 tej decyzji w związku z NZP 6 zawartym w załączniku II do tej decyzji, przyjęcie przez organizację zasad bezpiecznej przystani dokonywane jest w oparciu o system samocertyfikacji.

81 Jakkolwiek posłużenie się przez państwo trzecie systemem samocertyfikacji nie jest samo w sobie sprzeczne z wymogiem przewidzianym w art. 25 ust. 6 dyrektywy 95/46, zgodnie z którym odpowiedni stopień ochrony, który to państwo trzecie ma zapewnić, „wynika z […] prawa krajowego lub międzynarodowych zobowiązań" tego państwa, to jednak wiarygodność takiego systemu, w odniesieniu do tego wymogu, polega w istocie na wprowadzeniu skutecznych mechanizmów wykrywania i kontroli pozwalających na zidentyfikowanie i ukaranie w praktyce ewentualnych naruszeń reguł zapewniających ochronę praw podstawowych, w szczególności prawa do poszanowania życia prywatnego, a także prawa do ochrony danych osobowych.

82 W niniejszej sprawie zasady bezpiecznej przystani są – na mocy załącznika I akapit drugi decyzji 2000/520 – „przeznaczone do wyłącznego użytku przez amerykańskie organizacje otrzymujące dane osobowe z Unii Europejskiej, w celu zakwalifikowania ich jako »bezpiecznej przystani« i domniemania »odpowiedniego stopnia ochrony«, jaką ta przystań stwarza”. Zasady te mają zatem zastosowanie wyłącznie do organizacji amerykańskich, które dokonały samocertyfikacji, otrzymujących dane osobowe z Unii, przy czym nie wymaga się, aby władze publiczne Stanów Zjednoczonych zostały zobowiązane do poszanowania tych zasad.

83 Ponadto na mocy art. 2 decyzji 2000/520 decyzja ta „dotyczy jedynie adekwatności [odpowiedniego stopnia] ochrony zapewnianej w Stanach Zjednoczonych na mocy zasad [bezpiecznej przystani] wdrożonych zgodnie z NZP w celu spełnienia wymagań art. 25 ust. 1 dyrektywy [95/46]”, jednak nie zawiera wystarczających ustaleń co do środków, za pomocą których Stany Zjednoczone zapewniają odpowiedni stopień ochrony w rozumieniu art. 25 ust. 6 tej dyrektywy, jaki wynika z ich prawa krajowego lub międzynarodowych zobowiązań.

84 Dodatkowo, zgodnie z akapitem czwartym załącznika I do decyzji 2000/520, stosowanie omawianych zasad może być ograniczone w szczególności „wymaga[niami] bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa”, a także „ustawą, rozporządzeniem rządu albo prawem precedensowym, ustanawiającym sprzeczne obowiązki albo udzielającym wyraźnego upoważnienia, pod warunkiem że działając na mocy tego upoważnienia organizacja potrafi wykazać, że nieprzestrzeganie przez nią zasad jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych uzasadnionych interesów wspieranych przez to upoważnienie”.

85 W tym względzie w sekcji B załącznika IV do decyzji 2000/520 – w odniesieniu do ograniczeń, jakim poddane jest stosowanie zasad bezpiecznej przystani – podkreślono, że „[n]ajwyraźniej w przypadkach, gdy prawo amerykańskie nakłada sprzeczny obowiązek na organizacje amerykańskie, czy to działające w ramach »bezpiecznej przystani« czy poza nią, muszą one przestrzegać tego prawa”.

86 W ten sposób decyzja 2000/520 ustanawia pierwszeństwo „wymagań bezpieczeństwa narodowego, interesu publicznego albo przestrzegania [amerykańskiego] prawa” przed zasadami bezpiecznej przystani, pierwszeństwo, na mocy którego amerykańskie organizacje, które dokonały samocertyfikacji, otrzymujące dane osobowe z Unii, zobowiązane są odstąpić bez wyjątku od tych zasad, jeśli pozostają one w konflikcie z tymi wymogami i okazują się w związku z tym z nimi niezgodne.

87 Ze względu na powszechny charakter odstępstwa zawartego w akapicie czwartym załącznika I do decyzji 2000/520 odstępstwo to umożliwia w ten sposób ingerencję – opartą na wymaganiach bezpieczeństwa narodowego, interesu publicznego albo przestrzegania prawa – w prawa podstawowe osób, których dane osobowe zostały lub mogły zostać przekazane z Unii do Stanów Zjednoczonych. W tym względzie przy ustalaniu tego, czy mamy do czynienia z ingerencją w podstawowe prawo do poszanowania życia prywatnego, nie ma znaczenia, czy dane informacje związane z życiem prywatnym mają charakter wrażliwy, ani też to, czy ze względu na tę ingerencję zainteresowane osoby doświadczyły ewentualnych niedogodności (wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 33 i przytoczone tam orzecznictwo).

88 Ponadto decyzja 2000/520 nie zawiera żadnego stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób, których dane zostały przekazane z Unii do Stanów Zjednoczonych, ingerencji, które organy państwowe tego kraju mogłyby dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu, takiego jak bezpieczeństwo narodowe.

89 Dochodzi do tego okoliczność, że w decyzji 2000/520 nie ustalono istnienia skutecznej ochrony prawnej przed ingerencją tego rodzaju. Jak wskazał rzecznik generalny w pkt 204–206 opinii, mechanizmy postępowania przed Federalną Komisją Handlu – której kompetencje, opisane w szczególności w NZP 11 zawartym w załączniku II do tej decyzji, ograniczone są do sporów handlowych – oraz prywatnego arbitrażu dotyczą poszanowania przez amerykańskie przedsiębiorstwa zasad bezpiecznej przystani i nie mogą być realizowane w ramach sporów dotyczących zgodności z prawem ingerencji w prawa podstawowe wynikającej z działań państwowych.

90 Co więcej, powyższą analizę decyzji 2000/520 potwierdza dokonana przez Komisję ocena sytuacji wynikającej z wdrażania tej decyzji. W szczególności bowiem w pkt 2 i 3.2 komunikatu COM(2013) 846 final, a także w pkt 7.1, 7.2 i 8 komunikatu COM(2013) 847 final, przywołanych w pkt 13–16 i 22, 23 i 25 niniejszego wyroku, instytucja ta stwierdziła, że amerykańskie władze mogły uzyskiwać dostęp do danych osobowych przekazywanych z państw członkowskich do tego państwa i przetwarzać te dane w sposób niezgodny w szczególności z celami, do których owe dane zostały przekazane, oraz w szerszym zakresie niż ograniczony do tego, co absolutnie niezbędne i proporcjonalne dla bezpieczeństwa narodowego. Ponadto Komisja stwierdziła, że osobom, których dane dotyczą, nie przysługiwała droga prawna administracyjna ani sądowa umożliwiająca im uzyskanie dostępu do dotyczących ich danych i, w odpowiednim przypadku, uzyskania ich sprostowania lub usunięcia.

91 Jeśli chodzi o gwarantowany w Unii poziom ochrony podstawowych praw i wolności, uregulowania Unii stanowiące ingerencję w prawa podstawowe gwarantowane w art. 7 i 8 karty muszą, zgodnie z utrwalonym orzecznictwem Trybunału, zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostają dotknięte ingerencją, miały wystarczające gwarancje rzeczywistej ochrony ich danych przed ryzykiem nadużyć oraz uzyskaniem do nich bezprawnego dostępu i ich wykorzystywaniem. Konieczność zapewnienia takich gwarancji ma znaczenie tym większe, że dane osobowe przetwarzane są automatycznie i istnieje znaczne ryzyko bezprawnego uzyskania dostępu do nich (wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 54, 55 i przytoczone tam orzecznictwo).

92 Ponadto i przede wszystkim ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne (wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 52 i przytoczone tam orzecznictwo).

93 W ten sposób uregulowanie umożliwiające generalnie przechowywanie wszelkich danych osobowych wszystkich osób fizycznych, których dane zostały przekazane z Unii do Stanów Zjednoczonych 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 [zob. podobnie, w odniesieniu do dyrektywy 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 zmieniającej dyrektywę 2002/58/WE (Dz.U. L 105, s. 54), wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 57–61].

94 W szczególności uregulowanie pozwalające władzom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego, wynikającego z art. 7 karty (zob. podobnie wyrok Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 39).

95 Co więcej, 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 zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty. Artykuł 47 akapit pierwszy karty stanowi bowiem, że każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w tym artykule. Samo istnienie skutecznej kontroli sądowej służącej zapewnieniu poszanowania przepisów prawa Unii jest zatem nierozerwalnie związane z istnieniem państwa prawa (zob. podobnie wyroki: Les Verts/Parlament, 294/83, EU:C:1986:166, pkt 23; Johnston, 222/84, EU:C:1986:206, pkt 18, 19; Heylens i in., 222/86, EU:C:1987:442, pkt 14; a także UGT-Rioja i in. od C-428/06 do C-434/06, EU:C:2008:488, pkt 80).

96 Jak wskazano w pkt 71, 73 i 74 niniejszego wyroku, przyjęcie przez Komisję decyzji na podstawie art. 25 ust. 6 dyrektywy 95/46 wymaga prawidłowo uzasadnionego ustalenia przez tę instytucję, że dane państwo trzecie rzeczywiście zapewnia, ze względu na swoje ustawodawstwo wewnętrzne i zobowiązania międzynarodowe, poziom ochrony praw podstawowych merytorycznie równoważny poziomowi gwarantowanemu w unijnym porządku prawnym, jaki wynika w szczególności z powyższych punktów niniejszego wyroku.

97 Należy jednakże wskazać, że Komisja nie wykazała w swojej decyzji 2000/520, iż Stany Zjednoczone rzeczywiście „zapewniają” odpowiedni stopień ochrony ze względu na swoje ustawodawstwo lub zobowiązania międzynarodowe.

98 W konsekwencji, bez potrzeby badania zasad bezpiecznej przystani co do istoty, należy uznać, że art. 1 tej decyzji narusza wymogi ustanowione w art. 25 ust. 6 dyrektywy 95/46 w związku z kartą oraz że jest w związku z tym nieważny.

W przedmiocie art. 3 decyzji 2000/520

99 Z rozważań przedstawionych w pkt 53, 57 i 63 niniejszego wyroku wynika, że uwzględniając art. 28 dyrektywy 95/46 w związku w szczególności z art. 8 karty, krajowe organy nadzorcze powinny mieć możliwość rozpoznania w sposób całkowicie niezależny wszelkiej skargi dotyczącej ochrony praw i wolności osoby w odniesieniu do przetwarzania

dotyczących jej danych osobowych. Jest tak zwłaszcza w sytuacji, gdy przy okazji takiej skargi osoba wyraża wątpliwości co do zgodności decyzji Komisji przyjętej na podstawie art. 25 ust. 6 tej dyrektywy z ochroną życia prywatnego oraz wolności i praw podstawowych osób.

100 Tymczasem art. 3 ust. 1 akapit pierwszy decyzji 2000/520 przewiduje uregulowanie szczególne dotyczące kompetencji krajowych organów nadzorczych w odniesieniu do dokonanych przez Komisję ustaleń dotyczących odpowiedniego stopnia ochrony w rozumieniu art. 25 dyrektywy 95/46.

101 Zgodnie więc z owym przepisem organy te mogą „[b]ez uszczerbku dla ich uprawnień do podejmowania działania zmierzającego do zapewnienia zgodności z przepisami krajowymi przyjętymi na mocy przepisów innych niż art. 25 dyrektywy [95/46], […] wykonywać posiadane uprawnienia w celu zawieszenia przepływu danych do organizacji, która złożyła zaświadczenie o przestrzeganiu zasad [określonych w decyzji 2000/520]”, pod wymagającymi ścisłej interpretacji warunkami ustanawiającymi wysoki pułap przesłanek takiej interwencji. Jakkolwiek przepis ten nie narusza kompetencji tych organów do przyjęcia środków zmierzających do zapewnienia poszanowania przepisów krajowych przyjętych dla wdrożenia dyrektywy 95/46, to jednak wyklucza on kompetencje tych organów do przyjęcia środków zmierzających do zapewnienia poszanowania art. 25 tej dyrektywy.

102 Artykuł 3 ust. 1 akapit pierwszy decyzji 2000/520 należy zatem rozumieć jako pozbawiający krajowe organy nadzorcze ich kompetencji wynikających z art. 28 dyrektywy 95/46, w przypadku gdy przy okazji skargi wnoszonej na mocy tego przepisu jednostka przedstawia okoliczności mogące podważyć zgodność z ochroną życia prywatnego oraz wolnościami i prawami podstawowymi osób fizycznych decyzji Komisji stwierdzającej na podstawie art. 25 ust. 6 tej dyrektywy, że państwo trzecie zapewnia odpowiedni stopień ochrony.

103 Kompetencje wykonawcze przyznane przez prawodawcę Unii Komisji w art. 25 ust. 6 dyrektywy 95/46 nie umożliwiają tej instytucji ograniczenia kompetencji krajowych organów nadzorczych wymienionych w poprzednim punkcie niniejszego wyroku.

104 W tych okolicznościach należy stwierdzić, że przyjmując art. 3 decyzji 2000/520, Komisja przekroczyła granice kompetencji przyznanych jej w art. 25 ust. 6 dyrektywy 95/46 w związku z kartą, oraz że przepis ten jest z tego powodu nieważny.

105 Skoro art. 1 i 3 decyzji 2000/520 są nierozerwalnie związane z art. 2 i 4, a także z załącznikami do tej decyzji, nieważność art. 1 i 3 ma wpływ na ważność tej decyzji w całości.

106 W świetle wszystkich powyższych rozważań należy uznać, że decyzja 2000/520 jest nieważna.

W przedmiocie kosztów

107 Dla stron w postępowaniu głównym niniejsze postępowanie ma charakter incydentalny, dotyczy bowiem kwestii podniesionej przed sądem odsyłającym, do niego zatem należy rozstrzygnięcie o kosztach. Koszty poniesione w związku z przedstawieniem uwag Trybunałowi, inne niż koszty stron w postępowaniu głównym, nie podlegają zwrotowi.

Z powyższych względów Trybunał (wielka izba) orzeka, co następuje:

1) **Artykuł 25 ust. 6 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, zmienionej rozporządzeniem (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r., w związku z art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej należy interpretować w ten sposób, że decyzja przyjęta na podstawie tego przepisu, taka jak decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r., przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, w której Komisja Europejska stwierdza, że państwo trzecie zapewnia odpowiedni stopień ochrony, nie stoi na przeszkodzie temu, aby organ nadzorczy państwa członkowskiego, w rozumieniu art. 28 tej dyrektywy, w zmienionym brzmieniu, rozpatrzył skargę danej osoby związaną z ochroną jej praw i wolności w zakresie przetwarzania dotyczących jej danych osobowych, przekazanych z państwa członkowskiego do tego państwa trzeciego, gdy osoba ta podnosi, że prawo i praktyka obowiązujące w tym państwie trzecim nie zapewniają odpowiedniego stopnia ochrony.**

2) **Decyzja 2000/520 jest nieważna.**

Podpisy

Źródło: http://curia.europa.eu/