OPINIA RZECZNIKA GENERALNEGO PHILIPPE'A LÉGERA przedstawiona w dniu 22 listopada 2005 r. [1]

Spis treści

1 — Język oryginału: francuski.

1. Parlament Europejski wniósł do Trybunału na podstawie art. 230 WE dwie skargi o stwierdzenie nieważności. W sprawie C-317/04 Parlament przeciwko Radzie skarga dotyczy stwierdzenia nieważności decyzji Rady z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Ceł i Ochrony Granic [2]. W sprawie C-318/04 Parlament przeciwko Komisji Parlament wnosi o stwierdzenie nieważności decyzji Komisji z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Ceł i Ochrony Granic Stanów Zjednoczonych Ameryki [3].

2. Obydwie sprawy wymagają, by Trybunał rozstrzygał w zakresie problematyki związanej z ochroną danych osobowych pasażerów linii lotniczych, w sytuacji gdy w celu uzasadnienia przekazywania tych danych do państwa trzeciego i ich przetwarzania w państwie trzecim, w tym przypadku Stanach Zjednoczonych [4], przywoływane są nadrzędne względy bezpieczeństwa publicznego, wchodzące w zakres prawa karnego, takie jak zapobieganie terroryzmowi oraz innym poważnym przestępstwom i zwalczanie ich.

3. Obydwu sprawom początek dała seria zdarzeń, które należy teraz przedstawić. Następnie omówię ramy prawne, w które się one wpisują.

I — Okoliczności powstania sporu

4. Wkrótce po atakach terrorystycznych z dnia 11 września 2001 r. Stany Zjednoczone wydały przepisy zobowiązujące przewoźników lotniczych obsługujących loty do i ze Stanów Zjednoczonych oraz nad terytorium tego kraju do zapewnienia amerykańskim organom celnym elektronicznego dostępu do danych zawartych w ich automatycznych systemach rezerwacji i kontroli odlotów, tzw. Passenger Name Records (zwanych dalej „PNR") [5]. Komisja Wspólnot Europejskich, mimo iż uznała troskę

2 — Decyzja 2004/496/WE (Dz.U. L 183, str. 83, zwana dalej „decyzją Rady").

3 — Decyzja 2004/535/WE (Dz.U. L 235, str. 11, zwana dalej „decyzją o odpowiedniej ochronie").

4 — Problematyka ta dotyczy również stosunków Wspólnoty Europejskiej z innymi państwami trzecimi. Porozumienie podobnego rodzaju jak to będące przedmiotem sprawy C-317/04 zostało zawarte pomiędzy Wspólnotą Europejską a Kanadą w dniu 3 października 2005 r.

5 — Zobacz Aviation and Transportation Security Act (ATSA) z dnia 19 listopada 2001 r. [Public Law 107–71, 107th Congress, tytuł 49, sekcja 44909(c)(3) United States Code]. Do tej ustawy Biuro Ceł i Ochrony Granic amerykańskiego Ministerstwa Bezpieczeństwa Wewnętrznego (United States Bureau of Customs and Border Protection, zwane dalej „CBP") wydało akty wykonawcze, m.in. Passenger and Crew Manifests Required for Passengers Flights in Foreign Air Transportation to the United States, opublikowany w Federal Register (federalnym rejestrze amerykańskim) w dniu 31 grudnia 2001 r., oraz Passenger Name Record Information Required for Passengers on Flights in Foreign Air Transportation to or from the United States, opublikowany w Federal Register w dniu 25 czerwca 2002 r. (tytuł 19, sekcja 122.49b Code of Federal Regulations).

o zapewnienie bezpieczeństwa za w pełni zasadną, poinformowała jednak władze Stanów Zjednoczonych w czerwcu 2002 r., że te przepisy mogą stać w sprzeczności z ustawodawstwem wspólnotowym i państw członkowskich w zakresie ochrony danych osobowych oraz z pewnymi przepisami rozporządzenia w sprawie użytkowania komputerowych systemów rezerwacji (KSR) [6]. Władze Stanów Zjednoczonych przesunęły termin wejścia w życie nowych przepisów, ale odmówiły odstąpienia od stosowania sankcji wobec przedsiębiostw lotniczych, które się do nich nie zastosują po 5 marca 2003 r. Od tego momentu liczne duże przedsiębiorstwa lotnicze z państw członkowskich zapewniły władzom amerykańskim dostęp do swoich PNR.

5. Komisja rozpoczęła z władzami amerykańskimi negocjacje, w wyniku których został opracowany dokument zawierający zobowiązania ze strony CBP, co pozwoliło Komisji na wydanie decyzji stwierdzającej, że Stany Zjednoczone zapewniają odpowiedni poziom ochrony danych osobowych, zgodnie z art. 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 [7].

6. W dniu 13 czerwca 2003 r. grupa robocza ds. ochrony danych (tzw. grupa art. 29) [8] wydała opinię, w której wyraziła wątpliwości co do poziomu ochrony zapewnionego przez te zobowiązania przy zamierzonych sposobach przetwarzania danych [9]. Grupa ponownie przedstawiła swoje wątpliwości w kolejnej opinii z dnia 29 stycznia 2004 r. [10].

7. W dniu 1 marca 2004 r. Komisja wniosła do Parlamentu projekt decyzji o odpowiedniej ochronie wraz z projektem Zobowiązań CBP.

6 — Rozporządzenie Rady (EWG) nr 2299/89 z dnia 24 lipca 1989 r. w sprawie kodeksu postępowania dla komputerowych systemów rezerwacji (Dz.U. L 220, str.1), zmienione rozporządzeniem Rady (WE) nr 323/1999 z dnia 8 lutego 1999 r. (Dz.U. L 40, str. 1).

7 — Dz.U. L 281, str. 31, dyrektywa zmieniona rozporządzeniem (WE) nr 1882/2003 Parlamentu Europejskiego i Rady z dnia 29 września 2003 r. dostosowującym do decyzji Rady 1999/468/WE przepisy odnoszące się do komitetów, które wspomagają Komisję w wykonywaniu jej uprawnień wykonawczych ustanowionych w instrumentach podlegających procedurze określonej w art. 251 traktatu WE (Dz.U. L 284, str. 1).

8 — Grupa robocza została powołana na podstawie art. 29 dyrektywy nr 95/46. Jest to niezależny organ doradczy, działający w dziedzinie ochrony osób w zakresie przetwarzania danych osobowych. Jej zadania określa art. 30 wyżej wymienionej dyrektywy oraz art. 15 ust. 3 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201, str. 37).

9 — Opinia 4/2003 w sprawie poziomu ochrony zapewnionego przez Stany Zjednoczone przy transmisji danych pasażerów. Zobacz strona internetowa: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2003_fr.htm.

10 — Opinia 2/2004 w sprawie odpowiedniego poziomu ochrony danych osobowych zawartych w nazwie rekordu pasażera (PNR) przekazywanych do Biura Ceł i Ochrony Granic Stanów Zjednoczonych (US CBP). Zobacz strona internetowa: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2004_fr.htm.

8. W dniu 17 marca 2004 r. Komisja przekazała Parlamentowi projekt decyzji Rady Unii Europejskiej dotyczącej zawarcia umowy pomiędzy Wspólnotą a Stanami Zjednoczonymi celem przeprowadzenia konsultacji wymaganych przez art. 300 ust. 3 akapit pierwszy WE. Pismem z dnia 25 marca 2004 r. Rada zwróciła się do Parlamentu o wydanie opinii na temat tego projektu, w trybie pilnym przewidzianym przez art. 112 regulaminu Parlamentu (obecnie art. 134), najpóźniej do dnia 22 kwietnia 2004 r. W piśmie tym Rada podkreśliła, że „[w]alka z terroryzmem, uzasadniająca projektowane postanowienia, stanowi jeden z podstawowych priorytetów Unii Europejskiej. W chwili obecnej przewoźnicy lotniczy oraz pasażerowie znajdują się w sytuacji niepewności, której należy pilnie zapobiec. Dodatkowo należy chronić interesy finansowe podmiotów, których sprawa dotyczy".

9. W dniu 31 marca 2004 r. Parlament, na podstawie art. 8 decyzji Rady z dnia 28 czerwca 1999 r. ustanawiającej warunki wykonywania uprawnień wykonawczych przyznanych Komisji [11], przyjął uchwałę zawierającą szereg zastrzeżeń natury prawnej dotyczących proponowanego rozwiązania. W szczególności Parlament stwierdził, że projekt decyzji o odpowiedniej ochronie wykracza poza kompetencje powierzone Komisji na mocy art. 25 dyrektywy nr 95/46. Wezwał do zawarcia odpowiedniej umowy międzynarodowej zapewniającej poszanowanie praw podstawowych i zwrócił się do Komisji o przedłożenie mu nowego projektu decyzji. Zastrzegł sobie ponadto prawo do wystąpienia do Trybunału o zbadanie zgodności z prawem projektowanej umowy międzynarodowej, a w szczególności jej zgodności z prawem do poszanowania życia prywatnego.

10. W dniu 21 kwietnia 2004 r., na wniosek przewodniczącego, Parlament zatwierdził zalecenie komisji do spraw prawnych i rynku wewnętrznego, mówiące o konieczności zwrócenia się, na podstawie art. 300 ust. 6 WE, o opinię Trybunału w przedmiocie zgodności projektowanej umowy z postanowieniami traktatu. Postępowanie zostało wszczęte tego samego dnia. Parlament postanowił też, tego samego dnia, odesłać do komisji sprawozdanie o projekcie decyzji Rady, odrzucając tym samym na tym etapie w sposób dorozumiany wniosek Rady z dnia 25 marca 2004 r. o rozpatrzenie tego projektu w trybie pilnym.

11. W dniu 28 kwietnia 2004 r. Rada, na podstawie art. 300 ust. 3 akapit pierwszy WE, wystosowała do Parlamentu pismo, w którym zwróciła się do niego o wydanie opinii dotyczącej zawarcia umowy w terminie do dnia 5 maja 2004 r. Na uzasadnienie pilności sprawy powtórzyła argumenty zawarte w piśmie z dnia 25 marca 2004 r. [12].

11 — Decyzja 1999/468/WE (Dz.U. L 184, str. 23).

12 — Zobacz pkt 8 niniejszej opinii.

12. W dniu 30 kwietnia 2004 r. sekretarz Trybunału poinformował Parlament, że Trybunał wyznaczył termin do 4 czerwca 2004 r. na składanie uwag przez państwa członkowskie, Radę i Komisję w związku z wnioskiem o wydanie opinii nr 1/04.

13. W dniu 4 maja 2004 r. Parlament odrzucił wniosek Rady o rozpatrzenie w trybie pilnym, złożony w dniu 28 kwietnia [13]. Dwa dni później przewodniczący Parlamentu zwrócił się do Rady i Komisji, by powstrzymały się z realizacją swych zamierzeń do czasu wydania przez Trybunał opinii, o którą Parlament wystąpił w dniu 21 kwietnia 2004 r.

14. W dniu 14 maja 2004 r. Komisja wydała decyzję w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do CBP, zgodnie z art. 25 ust. 6 dyrektywy nr 95/46.

15. W dniu 17 maja 2004 r. Rada wydała decyzję dotyczącą zawarcia porozumienia pomiędzy Wspólnotą a Stanami Zjednoczonymi w sprawie przetwarzania i przekazywania danych PNR przez przewoźników lotniczych do CBP.

16. Pismem z dnia 9 lipca 2004 r. Parlament poinformował Trybunał o wycofaniu wniosku o wydanie opinii nr 1/04 [14]. Następnie postanowił wystąpić na drogę postępowania spornego w celu rozstrzygnięcia sporów pomiędzy nim a Radą i Komisją.

II — Ramy prawne obydwu spraw

A — *Traktat UE*

17. Zgodnie z art. 6 UE:

„1. Unia opiera się na zasadach wolności, demokracji, poszanowania praw człowieka i podstawowych wolności oraz państwa prawnego, które są wspólne dla państw członkowskich.

2. Unia szanuje prawa podstawowe zagwarantowane w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, podpisanej w Rzymie 4 listopada 1950 roku, oraz wynikające z tradycji kon-

13 — W złożonych skargach Parlament uzasadnia odrzucenie tego wniosku stwierdzeniem, iż w dalszym ciągu brakowało kompletu wersji językowych projektu decyzji Rady.

14 — Wniosek o wydanie opinii został wykreślony z rejestru Trybunału na podstawie postanowienia prezesa Trybunału z dnia 16 grudnia 2004 r.

stytucyjnych wspólnych dla państw członkowskich, jako zasady ogólne prawa wspólnotowego.

[...]".

B — *Traktat ustanawiający Wspólnotę Europejską*

18. Artykuł 95 ust. 1 WE stanowi:

„Na zasadzie odstępstwa od artykułu 94 i z zastrzeżeniem, że niniejszy traktat nie stanowi inaczej, do urzeczywistnienia celów określonych w artykule 14 stosuje się następujące postanowienia. Rada, stanowiąc zgodnie z procedurą określoną w artykule 251 i po konsultacji z Komitetem Ekonomiczno-Społecznym, przyjmuje środki dotyczące zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego".

19. Jeśli chodzi o procedurę zawierania umów międzynarodowych przez Wspólnotę, art. 300 ust. 2 akapit pierwszy WE przewiduje w pierwszym zdaniu, że „[z] zastrzeżeniem uprawnień przyznanych Komisji w tej dziedzinie, o podpisaniu [...], jak również o zawarciu umów decyduje Rada, stanowiąca większością kwalifikowaną na wniosek Komisji".

20. Artykuł 300 ust. 3 WE ma następujące brzmienie:

„Rada zawiera umowy po konsultacji z Parlamentem Europejskim, z wyjątkiem umów określonych w artykule 133 ustęp 3, włącznie z przypadkami, gdy umowa dotyczy dziedziny, w której do przyjęcia wewnętrznych przepisów wymagana jest procedura określona w artykule 251 lub określona w artykule 252. Parlament Europejski wyraża swoją opinię w terminie, który może ustalić Rada, stosownie do pilności sprawy. W przypadku braku opinii w tym terminie Rada może stanowić samodzielnie.

Na zasadzie odstępstwa od postanowień poprzedniego akapitu umowy określone w artykule 310, inne umowy, które tworzą specyficzne ramy instytucjonalne poprzez organizację procedur współpracy, umowy mające istotne implikacje budżetowe dla Wspólnoty oraz umowy powodujące zmianę aktu przyjętego według procedury określonej w artykule 251 są zawierane po uzyskaniu zgody Parlamentu Europejskiego.

Rada i Parlament Europejski mogą, w pilnych przypadkach, uzgodnić termin wyrażenia zgody".

C — *Europejskie prawo ochrony danych osobowych*

21. Artykuł 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności (zwanej dalej „EKPC") stanowi:

„1. Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji.

2. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób".

22. Europejskie prawo ochrony danych powstawało głównie w ramach Rady Europy. Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych została otwarta do podpisu dla państw członkowskich Rady Europy w Strasburgu w dniu 28 stycznia 1981 r. [15]. Celem tej konwencji jest zapewnienie każdej osobie fizycznej, bez względu na narodowość lub miejsce zamieszkania, poszanowania jej praw i podstawowych wolności na terytorium każdej z umawiających się stron, a w szczególności jej prawa do prywatności, w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych.

23. Jeśli chodzi o Unię Europejską, to poza art. 7, który dotyczy poszanowania życia prywatnego i rodzinnego, art. 8 Karty praw podstawowych Unii Europejskiej [16] został specjalnie poświęcony ochronie danych osobowych. Brzmienie tego artykułu jest następujące:

„1. Każda osoba ma prawo do ochrony danych osobowych, które jej dotyczą.

15 — Seria traktatów europejskich nr 108 (zwana dalej „konwencją nr 108"). Konwencja ta weszła w życie w dniu 1 października 1985 r. W dniu 15 czerwca 1999 r. Komitet Ministrów Rady Europy przyjął zmiany do konwencji w celu umożliwienia przystąpienia Wspólnot Europejskich (zmiany te do dnia dzisiejszego nie zostały zaakceptowane przez wszystkie państwa będące stronami konwencji nr 108). Zobacz także protokół zmieniający konwencję nr 108 dotyczący organów kontroli oraz przepływu danych przez granice. Protokół ten otwarto do podpisu w dniu 8 listopada 2001 r., a wszedł w życie w dniu 1 lipca 2004 r. (Seria traktatów europejskich, nr 181).

16 — Dz.U. 2000, C 364, str. 1. Karta, podpisana i proklamowana przez przewodniczących Parlamentu Europejskiego, Rady i Komisji podczas szczytu Rady Europejskiej w Nicei w dniu 7 grudnia 2000 r., figuruje w części II Traktatu ustanawiającego konstytucję dla Europy, na dzień dzisiejszy jeszcze nie obowiązującego (Dz.U. 2004, C 310, str. 41). Jak to zaznaczył Sąd Pierwszej Instancji Wspólnot Europejskich, „mimo iż prawnie nie ma mocy wiążącej, [Karta praw podstawowych Unii Europejskiej] wykazuje znaczenie praw, które wymienia, we wspólnotowym porządku prawnym". Zobacz wyrok z dnia 15 stycznia 2003 r. w sprawach połączonych T-377/00, T-379/00, T-380/00, T-260/01 i T-272/01 Philip Morris International i in. przeciwko Komisji, Rec. str. II-1, pkt 122).

2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każda osoba ma prawo dostępu do zebranych danych, które jej dotyczą, i prawo do dokonania ich sprostowania.

3. Przestrzeganie tych zasad podlega kontroli niezależnego organu".

24. Jeśli chodzi o prawo wspólnotowe pierwotne, art. 286 WE w ust. 1 przewiduje, że „[p]ocząwszy od 1 stycznia 1999 roku, akty wspólnotowe dotyczące ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych oraz swobodnego przepływu tych danych mają zastosowanie do instytucji i organów ustanowionych niniejszym traktatem lub na jego podstawie" [17].

25. W pochodnym prawie wspólnotowym podstawową regulację w tej dziedzinie stanowi dyrektywa nr 95/46 [18]. Jej powiązanie z aktami prawnymi Rady Europy wyraźnie wynika z motywów dziesiątego oraz jedenastego dyrektywy. W motywie dziesiątym stwierdza się mianowicie, że „[c]elem krajowych przepisów prawa dotyczących przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 [EKPC] [jak i] 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". Ponadto motyw jedenasty dyrektywy nr 95/46 wskazuje, że „[z]asady ochrony praw i wolności jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w konwencji [nr 108]".

26. Przyjęta na podstawie art. 100A traktatu WE (obecnie, po zmianie, art. 95 WE) dyrektywa 95/46 inspirowana była ideą wyrażoną w jej motywie trzecim, który stwierdza, że „[u]stanowienie i funkcjonowanie rynku wewnętrznego [...] wymaga nie tylko zapewnienia swobodnego przepływu danych osobowych z jednego państwa członkowskiego do drugiego, lecz

17 — Natomiast ust. 2 art. 286 WE brzmi następująco:
„Przed nadejściem daty określonej w ust. 1 Rada, stanowiąc zgodnie z procedurą określoną w artykule 251, ustanawia niezależny organ kontrolny odpowiedzialny za nadzorowanie stosowania tych aktów wspólnotowych do instytucji i organów wspólnotowych oraz, w odpowiednim przypadku, przyjmuje wszelkie inne właściwe przepisy".
Na podstawie art. 286 WE zostało przyjęte rozporządzenie 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, str. 1).

18 — W celu dokładniejszego poznania ogólnego kontekstu, w jakim była opracowywana dyrektywa i jej poszczególne przepisy zobacz: M.H. Boulanger, C. de Terwangne, T. Léonard, S. Louveaux, D. Moreau, Y. Poullet, „La protection des données à caractère personnel en droit communautaire", JTDE, 1997, nr 40, 41 i 42. Zobacz także: S. Simitis, „Data Protection in the European Union — the Quest for Common Rules" w: *Collected Courses of the Academy of European Law*, Volume VIII, Book I, 2001, str. 95. Nadmienię, iż istnieje również inna dyrektywa opracowana specjalnie w celu regulowania sektora łączności elektronicznej, tj. dyrektywa nr 2002/58.

również ochrony praw podstawowych osób fizycznych". Dokładniej rzecz ujmując punktem wyjścia ustawodawcy wspólnotowego było stwierdzenie, że „[r]óżnica w stopniu ochrony praw i wolności jednostek, szczególnie prawa do prywatności, w odniesieniu do przetwarzania danych osobowych zapewnionego w poszczególnych państwach członkowskich może uniemożliwiać przesyłanie tych danych z terytorium jednego państwa członkowskiego do drugiego państwa członkowskiego" [19], czego skutkiem mogą być w szczególności przeszkody w wykonywaniu działalności na skalę wspólnotową i zakłócenia konkurencji. Dlatego ustawodawca wspólnotowy uważał, że „[w] celu zniesienia przeszkód w przepływie danych osobowych stopień ochrony praw i wolności jednostek w zakresie przetwarzania tych danych musi być jednakowy we wszystkich państwach członkowskich" [20]. Zastosowanie takiego założenia powinno skutkować tym, że „[b]iorąc pod uwagę równoważną ochronę wynikającą ze zbliżania ustawodawstw krajowych, państwa członkowskie nie będą już mogły utrudniać między sobą swobodnego przepływu danych osobowych na podstawie ochrony praw i wolności jednostek, a zwłaszcza prawa do prywatności" [21].

27. Artykuł 1 dyrektywy 95/46, zatytułowany „Cel dyrektywy", wprowadza w życie te założenia w następujący sposób:

„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.

2. Państwa członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych między państwami członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1".

28. Artykuł 2 dyrektywy definiuje w szczególności pojęcia „danych osobowych", „przetwarzania danych osobowych" oraz „administratora danych".

29. Zgodnie z definicją zawartą w art. 2 lit. a) dyrektywy 95/46 do danych osobowych zaliczają się „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej [...]; 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".

19 — Motyw siódmy.
20 — Motyw ósmy.
21 — Motyw dziewiąty.

30. Przetwarzanie takich danych, według art. 2 lit. b) dyrektywy, obejmuje „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".

31. Artykuł 2 lit. d) dyrektywy 95/46 definiuje administratora danych jako „osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych [...]".

32. Jeśli chodzi o materialny zakres stosowania dyrektywy 95/46, art. 3 ust. 1 przewiduje, że dyrektywa „stosuje się do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych".

33. Artykuł 3 ust. 2 omawianej dyrektywy pozwala ustalić granice materialnego zakresu jej stosowania, stanowiąc że:

„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,

[...]".

34. Rozdział II dyrektywy 95/46 określa „Ogólne zasady legalności przetwarzania danych osobowych". W rozdziale tym przedmiotem sekcji I są „Zasady dotyczące jakości danych". Artykuł 6 tej dyrektywy wylicza te zasady określane jako zasady rzetelności,

legalności, celowości, proporcjonalności i prawidłowości przetwarzania danych osobowych. Jego brzmienie jest następujące:

„1. Państwa członkowskie zapewniają, aby dane osobowe były:

a) przetwarzane rzetelnie i legalnie;

b) gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem [...];

c) prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone;

d) prawidłowe oraz, w razie konieczności, aktualizowane [...];

e) przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane [...].

2. Na administratorze danych spoczywa obowiązek zapewnienia przestrzegania przepisów ust. 1".

35. Z kolei sekcja II rozdziału II dyrektywy ustala „Kryteria legalności przetwarzania danych". Artykuł 7, tworzący tę sekcję, ma następujące brzmienie:

„Państwa członkowskie zapewniają, że dane osobowe mogą być przetwarzane tylko wówczas, gdy:

a) osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę; lub

b) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy; lub

c) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega

[...]".

36. Jeśli chodzi o dane osobowe potocznie określane jako wrażliwe, art.8 ust. 1 wprowadza jako zasadę zakaz ich przetwarzania. Przewiduje on mianowicie, że „[p]aństwa członkowskie zabraniają przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również przetwarzanie danych dotyczących zdrowia i życia seksualnego". Od tego zakazu przewidziano jednak liczne wyjątki, których treść i zasady stosowania są określone w następnych ustępach tego artykułu.

37. Zgodnie z art. 13 ust. 1 dyrektywy 95/46, zatytułowanego „Zwolnienia i ograniczenia":

„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 Europejskiej, 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".

38. Równocześnie ustawodawca wspólnotowy chciał, żeby stworzony w ten sposób system ochrony nie został obrócony wniwecz, w momencie gdy dane osobowe opuszczają terytorium Wspólnoty. Okazało się bowiem, że międzynarodowy zasięg przepływu informacji [22] sprawi, iż regulacje obejmujące swoim działaniem tylko to terytorium staną się niewystarczające, a wręcz bezużyteczne. Dlatego ustawodawca wspólnotowy zdecydował się na system wymagający, przed dopuszczeniem do transferu danych osobowych do państwa trzeciego, aby państwo to zapewniło danym „odpowiedni stopień ochrony".

39. W konsekwencji ustawodawca wspólnotowy wprowadził zasadę, zgodnie z którą „należy zakazać przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony" [23].

40. W związku z powyższym art. 25 dyrektywy 95/46 określa zasady, jakim podlega przekazywanie danych osobowych państwom trzecim:

„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

22 — Tytułem przykładu można tu wymienić przepływy danych związane z mobilnością osób, handlem elektronicznym oraz transmisją danych w obrębie grupy przedsiębiorstw.

23 — Motyw pięćdziesiąty siódmy dyrektywy 95/46.

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 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".

41. Na koniec należy zaznaczyć, że w ramach tytułu VI traktatu UE, dotyczącego współpracy policyjnej i sądowej w sprawach karnych, kwestie ochrony danych osobowych reguluje kilka szczególnych aktów prawnych. Są to w szczególności akty, na podstawie których utworzono wspólne systemy informacyjne na szczeblu europejskim, takie jak Konwencja wykonawcza do układu z Schengen [24], która zawiera postanowienia szczególne dotyczące ochrony danych w Systemie Informacyjnym Schengen (SIS) [25]; Konwencja sporządzona na podstawie art. K.3 Traktatu o Unii Europejskiej w sprawie utworzenia europejskiego urzędu policji [26]; decyzja Rady o utworzeniu Eurojustu [27] oraz przepisy regulaminu wewnętrznego Eurojustu dotyczące przetwarzania i ochrony danych osobowych [28]; Konwencja sporządzona na podstawie art. K.3 Traktatu o Unii Europejskiej w sprawie wykorzystania technologii informatycznych do celów odpraw celnych, która zawiera postanowienia o ochronie danych osobowych mające zastosowanie do systemu informacji celnej [29] oraz Konwencja o wzajemnej pomocy w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej [30].

42. W dniu 4 października 2005 r. Komisja przedstawiła projekt decyzji ramowej Rady

24 — Konwencja wykonawcza do układu z Schengen z dnia 14 czerwca 1985 roku między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, podpisana w Schengen w dniu 19 czerwca 1990 r. (Dz.U. 2000, L 239, str. 19).

25 — Zobacz art. 102–118 wyżej wymienionej konwencji. Jeśli chodzi o System Informacyjny Schengen drugiej generacji (SIS II), Komisja przedstawiła projekty aktów, które mają być przyjęte przez Radę: decyzji [COM(2005) 230 wersja ostateczna] oraz dwóch rozporządzeń [COM(2005) 236 wersja ostateczna i COM(2005) 237 wersja ostateczna].

26 — Dz.U. 1995, C 316, str. 2, zwana dalej „konwencją o Europolu".

27 — Decyzja 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością (Dz.U. L 63, str. 1, zwana dalej „decyzją o Eurojuście"). Zobacz art. 14 i nast. wyżej wymienionej decyzji.

28 — Dz.U. 2005, C 68, str. 1.

29 — Dz.U. 1995, C 316, str. 34. Zobacz w szczególności art. 13–15, 17 oraz 18 wyżej wymienionej konwencji.

30 — Akt Rady z dnia 29 maja 2000 r. ustanawiający tę konwencję, zgodnie z art. 34 Traktatu o Unii Europejskiej (Dz.U. 2000, C 197, str. 1). Zobacz w szczególności art. 23 konwencji.

w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych [31].

„[w] takim przypadku dane osobowe można przekazywać z państw członkowskich bez konieczności zapewniania dodatkowych gwarancji".

III — Zaskarżone decyzje

43. Zaskarżone decyzje zbadam według porządku chronologicznego ich przyjęcia.

A — *Decyzja o odpowiedniej ochronie*

44. Decyzja o odpowiedniej ochronie została przyjęta przez Komisję na podstawie art. 25 ust. 6 dyrektywy 95/46, który — przypominam — upoważnia ją do stwierdzenia, że państwo trzecie zapewnia odpowiedni poziom ochrony danych osobowych [32]. Jak zaznaczono w motywie drugim tej decyzji

45. W motywie jedenastym omawianej decyzji Komisja wskazuje, że: „[p]rzetwarzanie przez CBP przekazywanych mu danych osobowych zawartych w PNR pasażerów lotniczych regulują warunki określone w Zobowiązaniach Ministerstwa Bezpieczeństwa Wewnętrznego Biura Celnego i Ochrony Granic (Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection) (CBP) z dnia 11 maja 2004 r. (zwanych dalej »Zobowiązaniami«) oraz prawodawstwo Stanów Zjednoczonych w zakresie przewidzianym w Zobowiązaniach". W motywie czternastym tejże decyzji Komisja stwierdza, że „[n]ormy, zgodnie z którymi CBP będzie przetwarzać zawarte w PNR dane osobowe pasażerów, na podstawie prawodawstwa Stanów Zjednoczonych oraz Zobowiązań uwzględniają podstawowe zasady niezbędne dla zapewnienia odpowiedniego poziomu ochrony osób fizycznych".

46. W związku z powyższym art. 1 decyzji o odpowiedniej ochronie stanowi:

„Dla celów art. 25 ust. 2 dyrektywy 95/46/WE Biuro Ceł i Ochrony Granic Stanów Zjednoczonych (dalej zwane jako CBP) traktowane jest jako zapewniające odpo-

31 — COM(2005) 475 wersja ostateczna. Ten projekt decyzji ramowej oparty jest na art. 30 UE, 31 UE oraz 34 ust. 2 lit. b) UE. Stanowi ona jeden ze środków przewidzianych w planie działania Rady i Komisji służącym realizacji programu haskiego mającego na celu wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej (Dz.U. 2005, C 198, str. 1, pkt 3.1).

32 — Jeśli chodzi o środki wykonawcze do dyrektywy 95/46, to decyzja o odpowiedniej ochronie została wydana w trybie określonym w art. 31 ust. 2 dyrektywy, który z kolei wymaga zastosowania art. 4, 7 i 8 decyzji 1999/468. Tak więc przy przyjmowaniu środków wykonawczych do wyżej wymienionej dyrektywy Komisję wspiera komitet, w którego skład wchodzą przedstawiciele państw członkowskich, a przewodniczy mu przedstawiciel Komisji. W omawianym przypadku jest to tzw. komitet artykułu 31.

wiedni poziom ochrony danych zawartych w PNR przekazywanych ze Wspólnoty na temat lotów do lub ze Stanów Zjednoczonych, zgodnie ze Zobowiązaniami określonymi w Załączniku".

47. Ponadto art. 3 decyzji o odpowiedniej ochronie przewiduje, że przekazywanie danych do CBP może zostać zawieszone przez właściwe organy państw członkowskich na następujących zasadach:

„1. Bez uszczerbku dla uprawnień umożliwiających podjęcie działań w celu zagwarantowania przestrzegania przepisów krajowych przyjętych zgodnie z przepisami innymi niż zawarte w art. 25 dyrektywy 95/46/WE właściwe władze państw członkowskich mogą wykonywać obecne uprawnienia w celu zawieszenia przepływu danych do CBP w celu ochrony osób fizycznych odnośnie do przetwarzania ich danych osobowych w jednym z poniższych przypadków:

a) gdy właściwy organ Stanów Zjednoczonych ustalił, że CBP narusza obowiązujące normy ochrony; lub

b) gdy istnieje wysokie prawdopodobieństwo, że normy ochrony określone w Załączniku są naruszane; gdy istnieją uzasadnione podstawy, aby domniemywać, iż CBP nie podejmuje lub nie podejmie odpowiednich i natychmiastowych kroków zmierzających do rozstrzygnięcia sprawy; gdy dalsze przekazywanie danych spowodowałoby realne niebezpieczeństwo wyrządzenia szkody osobom, których dotyczą dane osobowe, a właściwe organy w państwie członkowskim podjęły, odpowiednie w tych okolicznościach, wysiłki w celu dostarczenia CBP powiadomienia o powyższym oraz umożliwienia mu udzielenia odpowiedzi.

2. Zawieszenie ustaje, gdy tylko zapewnione zostaną normy ochrony, a właściwe organy danych państw członkowskich zostaną o tym powiadomione".

48. Państwa członkowskie są zobowiązane informować Komisję o środkach podjętych na mocy art. 3 decyzji o odpowiedniej ochronie. Ponadto państwa członkowskie i Komisja, zgodnie z art. 4 ust. 2 decyzji, powinny informować się wzajemnie o każdej zmianie w normach ochrony oraz o przypadkach, w których normy te wydają się niewystarczająco przestrzegane. W związku z wymianą informacji art. 4 ust. 3 decyzji o odpowiedniej ochronie przewiduje, że „[j]eżeli informacje zebrane zgodnie z art. 3 oraz zgodnie z ust. 1 i 2 niniejszego artykułu wykazują, że podstawowe zasady niezbędne do zapewnienia odpowiedniego poziomu ochrony osób fizycznych nie są już przestrzegane lub że jakikolwiek organ odpowie-

dzialny za przestrzeganie przez CBP norm ochrony ustanowionych w Załączniku nie spełnia swojej roli, CBP jest o tym informowane i, w razie potrzeby, stosuje się procedurę określoną w art. 31 ust. 2 dyrektywy 95/46/WE w celu uchylenia lub zawieszenia niniejszej decyzji".

49. Równocześnie art. 5 decyzji o odpowiedniej ochronie wprowadza zasadę, zgodnie z którą realizacja tej decyzji będzie poddawana ocenie, oraz przewiduje, że „wszelkie istotne informacje zostaną przekazane komitetowi powołanemu na mocy art. 31 dyrektywy 95/46/WE".

50. Ponadto art. 7 decyzji o odpowiedniej ochronie stanowi, że decyzja ta „wygasa trzy lata i sześć miesięcy od dnia jej notyfikacji, chyba że zostanie przedłużona zgodnie z procedurą określoną w art. 31 ust. 2 dyrektywy 95/46/WE".

51. Do omawianej decyzji załączony został tekst Zobowiązań CBP, we wstępie do którego stwierdza się, iż służą one do „poparcia planu" Komisji zmierzającego do uznania, że odpowiednia ochrona danych przekazywanych do CBP jest zapewniona. Zgodnie z tym co zostało w nich stwierdzone, Zobowiązania, zawierające w sumie 48 punktów, „nie tworzą ani nie przyznają żadnych praw lub korzyści osobom lub stronom tak prywatnym, jak i publicznym" [33].

52. W wywodach przestawionych w dalszej części wskażę treść zobowiązań istotnych dla rozstrzygnięcia sporu.

53. Decyzja o odpowiedniej ochronie zawiera także załącznik A, w którym wyliczono 34 elementy danych zawartych w PNR wymaganych przez CBP od przedsiębiorstw lotniczych [34].

54. W ślad za decyzją Komisji została wydana decyzja Rady w sprawie zawarcia porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi.

33 — Zobacz pkt 47 Zobowiązań.

34 — Są to następujące elementy: „1. Numer rezerwacji PNR; 2. Data rezerwacji; 3. Data/y planowanej podróży; 4. Nazwisko; 5. Inne nazwiska/imiona zawarte w PNR; 6. Adres; 7. Wszelkie informacje dotyczące płatności; 8. Adres na rachunku; 9. Kontaktowe numery telefonu; 10. Trasa całej podróży dla określonego PNR; 11. Informacje dotyczące osoby często podróżującej (ograniczone do ilości przelecianych mil i adresu(-ów)); 12. Biuro podróży; 13. Agent biura podróży; 14. Kod dzielonej informacji PNR; 15. Status podróżny pasażera (Travel status); 16. Podzielona informacja PNR; 17. Adres elektroniczny (e-mail); 18. Informacje na temat wystawienia biletu; 19. Uwagi ogólne; 20. Numer biletu; 21. Numer miejsca; 22. Data wystawienie biletu; 23. Niepojawienie się pasażera, który dokonał rezerwacji (No show); 24. Numer przywieszki bagażowej; 25. Informacja o pasażerze, który nie dokonał uprzedniej rezerwacji (Go show information); 26. Informacja OSI (inn[e] usług[i]); 27. Informacja SSI/SSR (specjalne usługi); 28. Otrzymane z informacji; 29. Wszystkie zmiany wprowadzone do PNR; 30. Liczba podróżujących w ramach danego PNR; 31. Informacja na temat miejsca; 32. Bilety w jedną stronę; 33. Wszelkie zebrane informacje APIS (Advanced Passenger Information System); 34. Pola ATFQ (Automatic Ticketing Fare Quote)".

B — *Decyzja Rady*

55. Decyzja Rady została przyjęta na podstawie art. 95 w związku z art. 300 ust. 2 akapit pierwszy zdanie pierwsze WE.

56. Motyw pierwszy tej decyzji stwierdza, że „[d]nia 23 lutego 2004 r. Rada upoważniła Komisję do negocjowania w imieniu Wspólnoty Porozumienia ze Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do [CBP]" [35]. Z kolei w motywie drugim decyzji zaznaczono, że „Parlament Europejski nie przedstawił swojej opinii w terminie wyznaczonym zgodnie z pierwszym akapitem art. 300 ust. 3 traktatu przez Radę w związku z pilną potrzebą zapobieżenia sytuacji niepewności, w której znajdują się linie lotnicze i pasażerowie, i ochrony interesów finansowych zainteresowanych podmiotów".

57. Na mocy art. 1 decyzji Rady porozumienie zostaje zatwierdzone w imieniu Wspólnoty. Ponadto art. 2 decyzji upoważnia przewodniczącego Rady do wyznaczenia osoby lub osób uprawnionych do podpisania porozumienia w imieniu Wspólnoty.

35 — Zwane dalej „porozumieniem".

58. Tekst porozumienia jest załączony do omawianej decyzji Rady. Artykuł 7 porozumienia przewiduje, że wchodzi ono w życie po jego podpisaniu. Zgodnie z tym artykułem porozumienie podpisane w Waszyngtonie w dniu 28 maja 2004 r. weszło w życie tego samego dnia [36].

59. W preambule porozumienia Wspólnota i Stany Zjednoczone uznają „znaczenie poszanowania podstawowych praw i wolności, w szczególności prywatności, oraz znaczenie poszanowania tych wartości podczas zapobiegania i zwalczania terroryzmu i związanych z nim przestępstw oraz innych poważnych przestępstw o ponadnarodowym charakterze, włącznie z przestępczością zorganizowaną".

60. W preambule porozumienia przywołane zostały następujące akty prawne: dyrektywa 95/46, a w szczególności jej art. 7 lit. c), Zobowiązania CBP oraz decyzja o odpowiedniej ochronie [37].

36 — Zobacz informacja dotycząca daty wejścia w życie Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dotyczących nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Ceł i Ochrony Granic (Dz.U. 2004, C 158, str. 1).

37 — Należy zaznaczyć, że preambuła porozumienia błędnie przywołuje decyzję o odpowiedniej ochronie. Faktycznie chodzi bowiem o decyzję 2004/535/WE z dnia 14 maja 2004 r. ogłoszoną pod numerem C(2004) 1914, a nie o decyzję C(2004) 1799 z 17 maja 2004 r. Sprostowanie tej pomyłki zostało opublikowane w *Dzienniku Urzędowym Unii Europejskiej* [zob. Protokół ze sprostowania do porozumienia (Dz.U. 2005, L 255, str. 168)].

61. Strony porozumienia zwracają również uwagę, że „przewoźnicy lotniczy z systemami kontroli rezerwacji/odlotów znajdującymi się na terytorium państw członkowskich Wspólnoty Europejskiej powinni zająć się transmisją danych dot. nazwy rekordu pasażera (PNR) do Biura Ceł i Ochrony Granic (CBP) kiedy tylko będzie to możliwe pod względem technicznym, jednak do tego czasu władze Stanów Zjednoczonych powinny mieć prawo bezpośredniego dostępu do tych danych, zgodnie z przepisami tego porozumienia" [38].

62. W związku z tym pkt 1 porozumienia przewiduje, że „(CBP) posiada elektroniczny dostęp do danych dot. nazwy rekordu pasażera (PNR) pochodzących z systemów kontroli rezerwacji/odlotów przewoźników lotniczych [...] znajdujących się na terytoriach państw członkowskich Wspólnoty Europejskiej w ścisłej zgodności z decyzją [39] i tak długo dopóki decyzja ma zastosowanie [czyli] jedynie do momentu kiedy wprowadzenia zadowalającego systemu pozwalającego na przekazywanie takich danych przez przewoźników lotniczych".

63. Obok uprawnienia zapewniającego CBP bezpośredni dostęp do danych PNR pkt 2 porozumienia nakłada na przewoźników lotniczych świadczących usługi międzynarodowego przewozu pasażerów do i ze Stanów Zjednoczonych, obowiązek przetwarzania danych PNR przechowywanych w ich informatycznych systemach rezerwacji „zgodnie z wymaganiami Biura Ceł i Ochrony Granic (CBP) odpowiednio do prawa Stanów Zjednoczonych i w ścisłej zgodności z decyzją [40] oraz tak długo dopóki decyzja ma zastosowanie".

64. Ponadto pkt 3 porozumienia uściśla, że CBP „przyjmuje do wiadomości" decyzję o odpowiedniej ochronie i „stwierdza, że wprowadza w życie zobowiązania załączone do niej". Dodatkowo pkt 4 omawianego porozumienia przewiduje, że „Biuro Ceł i Ochrony Granic (CBP) przetwarza otrzymane dane i traktuje przedmiot danych objętych takim przetwarzaniem zgodnie z obowiązującym prawem Stanów Zjednoczonych oraz wymaganiami konstytucyjnymi, bez bezprawnej dyskryminacji, w szczególności dyskryminacji ze względu na przynależność państwową i kraj zamieszkania".

65. Ponadto CBP i Wspólnota zobowiązują się wspólnie i regularnie dokonywać przeglądów wprowadzania w życie porozumienia [41]. Przewiduje ono również, że „[w] przypadku kiedy w Unii Europejskiej zostanie wprowadzony system identyfikacji pasażerów linii lotniczej wymagający od przewoźników lotniczych udostępnienia władzom danych dot. nazwy rekordu pasażera (PNR) osób, których trasy przelotów obejmują obecnie przelot do lub z Unii Europejskiej, Departa-

38 — Przekazywanie danych przez przewoźników lotniczych odbywa się w systemie „push", natomiast bezpośredni dostęp dla CBP do tych danych opiera się na systemie „pull".

39 — Chodzi o decyzję o odpowiedniej ochronie, jedyną „decyzję", o której mowa w preambule porozumienia.

40 — Taka sama uwaga jak w poprzednim przypisie.

41 — Punkt 5 porozumienia.

ment Bezpieczeństwa Wewnętrznego [Department of Homeland Security, DHS], jeśli tylko ma to zastosowanie i ściśle w oparciu o zasadę wzajemności, aktywnie promuje współpracę linii lotniczych w ramach swojej właściwości" [42].

66. Dodatkowo pkt 7 porozumienia, poza ustaleniem, że wchodzi ono w życie po podpisaniu, przewiduje także, że każda ze stron może je wypowiedzieć w dowolnym czasie. W takim przypadku porozumienie przestaje obowiązywać 90 dni od dnia notyfikowania wypowiedzenia drugiej stronie. Ponadto w tym samym punkcie przewidziano, że porozumienie może być zmienione w dowolnym czasie za wspólną zgodą stron wyrażoną na piśmie.

67. Wreszcie pkt 8 porozumienia stanowi, że „[c]elem tego porozumienia nie jest ani uchylenie, ani zmiana ustawodawstwa stron, ani również stworzenie lub przyznanie jakiegokolwiek prawa czy korzyści jakiejkolwiek osobie lub podmiotowi, prywatnemu albo publicznemu".

42 — Punkt 6 porozumienia.

IV — Zarzuty podniesione przez Parlament Europejski w niniejszych sprawach

68. W sprawie C-317/04 Parlament zgłosił sześć zarzutów do decyzji Rady:

— błędny wybór art. 95 WE jako podstawy prawnej;

— naruszenie art. 300 ust. 3 akapit drugi WE przez zmianę dyrektywy 95/46;

— naruszenie prawa do ochrony danych osobowych;

— naruszenie zasady proporcjonalności;

— niedostateczne uzasadnienie spornej decyzji;

— naruszenie zasady lojalnej współpracy, o której mowa w art. 10 WE.

69. Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Komisja zostały dopuszczone do udziału w postępowaniu w charakterze interwenientów po stronie Rady [43]. Równocześnie Europejski Inspektor Ochrony Danych (zwany dalej „EIOD") został dopuszczony do udziału w postępowaniu w charakterze interwenienta po stronie Parlamentu [44].

70. W sprawie C-318/04 Parlament zgłosił cztery zarzuty do decyzji o odpowiedniej ochronie:

— nadużycie władzy;

— naruszenie podstawowych zasad dyrektywy 95/46;

— naruszenie praw podstawowych;

— naruszenie zasady proporcjonalności.

71. Zjednoczone Królestwo zostało dopuszczone do udziału w postępowaniu w charakterze interwenienta po stronie Komisji [45]. Ponadto EIOD został dopuszczony do udziału w postępowaniu w charakterze interwenienta po stronie Parlamentu [46].

72. Przeanalizuję niniejsze dwie skargi w takiej kolejności, w jakiej zaskarżone decyzje zostały przyjęte. W związku tym najpierw zajmę się skargą o stwierdzenie nieważności decyzji o odpowiedniej ochronie (sprawa C-318/04), a w drugiej kolejności skargą o stwierdzenie nieważności decyzji Rady (sprawa C-317/04).

V — W przedmiocie skargi o stwierdzenie nieważności decyzji o odpowiedniej ochronie (sprawa C-318/04)

A — *W przedmiocie zarzutu nadużycia przez Komisję władzy przez wydanie decyzji o odpowiedniej ochronie*

1. Argumenty stron

73. Na poparcie tego zarzutu Parlament podnosi argument, że po pierwsze decyzja

43 — Postanowienia prezesa Trybunału odpowiednio z dnia 18 stycznia 2005 r. i 18 listopada 2004 r.

44 — Postanowienie Trybunału z dnia 17 marca 2005 r.

45 — Postanowienie prezesa Trybunału z dnia 17 grudnia 2004 r.

46 — Postanowienie Trybunału z dnia 17 marca 2005 r.

o odpowiedniej ochronie, w zakresie w jakim służy realizacji określonego celu w dziedzinie bezpieczeństwa publicznego oraz prawa karnego, narusza dyrektywę 95/46, ponieważ odnosi się do dziedziny wyłączonej z zakresu stosowania ratione materiae omawianej dyrektywy. To wyłączenie zostało wyraźnie określone w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 i nie może być w żadnym razie interpretowane w sposób ograniczający jego zakres. Fakt, iż dane osobowe były gromadzone przy wykonywaniu działalności gospodarczej, tj. sprzedaży biletów lotniczych uprawniających do skorzystania z usługi, nie może uzasadniać zastosowania omawianej dyrektywy, a w szczególności jej art. 25, w dziedzinie wyłączonej z jej zakresu stosowania.

74. Po drugie, Parlament utrzymuje, że CBP nie jest państwem trzecim w rozumieniu art. 25 dyrektywy 95/46. Artykuł ten w ust. 6 wprowadza wymóg, by decyzja Komisji stwierdzająca zapewnienie prawidłowego poziomu ochrony dotyczyła „państwa trzeciego", czyli państwa lub podmiotu traktowanego na równi z państwem, a nie organu administracyjnego lub jednostki organizacyjnej organu administracji wchodzącego w skład władzy wykonawczej państwa.

75. Po trzecie, Parlament uważa, że wydanie przez Komisję decyzji o odpowiedniej ochronie stanowi nadużycie władzy, gdyż załączony do niej tekst Zobowiązań wyraźnie zezwala na przekazywanie przez CBP danych PNR innym organom rządowym amerykańskim lub zagranicznym.

76. Po czwarte, Parlament stoi na stanowisku, że decyzja o odpowiedniej ochronie wprowadza pewne ograniczenia i wyjątki od zasad ujętych w dyrektywie 95/46, podczas gdy art. 13 dyrektywy zastrzega to uprawnienie wyłącznie dla państw członkowskich. Toteż przyjmując decyzję o odpowiedniej ochronie, Komisja podjęła działanie w miejsce państw członkowskich i w ten sposób naruszyła art. 13 tej dyrektywy. Wydając akt wykonawczy do dyrektywy 95/46 Komisja weszła w zakres kompetencji ściśle zastrzeżonych dla państw członkowskich.

77. Po piąte, Parlament argumentuje, że udostępnienie danych w oparciu o system „pull" (pobieranie danych) nie jest „przekazywaniem" w rozumieniu art. 25 dyrektywy 95/46, a zatem nie powinno być dopuszczone.

78. Jako ostatni argument podniesiono, że ze względu na wzajemne zależności między decyzją o odpowiedniej ochronie a porozumieniem rzeczona decyzja powinna, według tej instytucji, być uważana za środek nieodpowiedni do celu nałożenia obowiązku przekazywania danych PNR.

79. W odróżnieniu od Parlamentu EIOD stoi na stanowisku, że zapewnienie dostępu do danych osobie lub instytucji z państwa trzeciego może być traktowane jako mieszczące się w pojęciu przekazywania i że w związku z tym art. 25 dyrektywy 95/46 ma tutaj zastosowanie. Inspektor uważa też, że ograniczanie pojęcia do przekazywania przez podmiot wysyłający pozwoliłoby na obejście zasad ustalonych w tym artykule i w ten sposób osłabiłoby ochronę danych przewidzianą przez tenże artykuł.

80. Komisja, popierana przez Zjednoczone Królestwo, jest zdania, że działalność przewoźników lotniczych wchodzi w zakres stosowania prawa wspólnotowego, a w konsekwencji dyrektywa 95/46 ma tu w pełni zastosowanie. System stworzony w ramach przekazywania danych PNR nie dotyczy działalności państwa członkowskiego ani władz publicznych, niewchodzącej w zakres zastosowania prawa wspólnotowego.

81. Ponadto Komisja podnosi argument, że porozumienie zostało zawarte w imieniu Stanów Zjednoczonych, a nie w imieniu jednej z agend rządowych. Jeśli chodzi o dalsze przekazywanie danych PNR przez CBP Komisja uważa, że ochrona danych osobowych nie jest nie do pogodzenia z wyrażeniem zgody na ich dalsze przekazywanie, pod warunkiem że zostanie ono poddane odpowiednim i koniecznym ograniczeniom.

82. Na koniec Komisja zwraca uwagę, iż art. 13 dyrektywy 95/46 nie ma związku z niniejszą sprawą oraz że „przekazywanie" w rozumieniu art. 25 dyrektywy stanowi dla przewoźników lotniczych aktywne udostępnienie CBP danych PNR. Rozpatrywany system obejmuje więc przekazywanie danych w rozumieniu dyrektywy 95/46.

2. Ocena

83. W pierwszym zarzucie Parlament podnosi argument, że decyzja o odpowiedniej ochronie stanowi naruszenie dyrektywy 95/46, a w szczególności jej art. 3 ust. 2, art. 13 i 25. Utrzymuje zwłaszcza, że decyzja ta nie mogła być zgodnie z prawem wydana w oparciu o omawianą dyrektywę jako akt podstawowy.

84. Jak już mówiłem, dyrektywa 95/46 ma na celu — w związku z ustanowieniem i funkcjonowaniem rynku wewnętrznego — zniesienie przeszkód dla swobodnego przepływu danych osobowych przez zapewnienie we wszystkich państwach członkowskich jednakowego poziomu ochrony praw i wolności osób w zakresie przetwarzania tych danych.

85. Ustawodawca wspólnotowy chciał również, by stworzony w ten sposób system ochrony nie został zagrożony, w momencie gdy dane osobowe opuszczają terytorium Wspólnoty. Dlatego zdecydował się na system wymagający dla uznania, że transfer danych osobowych do państwa trzeciego może być zrealizowany, aby państwo to zapewniło danym odpowiedni stopień ochrony. W efekcie dyrektywa 95/46 zawiera zasadę, zgodnie z którą należy zakazać przekazywania danych osobowych do państwa trzeciego, które nie zapewnia odpowiedniego stopnia ochrony.

86. Artykuł 25 omawianej dyrektywy nakłada na państwa członkowskie i Komisję szereg obowiązków związanych z kontrolowaniem przekazywania danych osobowych do państw trzecich z uwzględnieniem stopnia ochrony tych danych zapewnionego w każdym z tych państw. Określa również metodę i kryteria pozwalające ustalić, czy państwo trzecie zapewnia odpowiedni stopień ochrony przekazywanych mu danych osobowych.

87. Trybunał określił system związany z przekazywaniem danych osobowych do państw trzecich jako „specyficzny system zawierający specyficzne zasady, służący zapewnieniu kontroli przez państwa członkowskie nad przekazywaniem danych osobowych do państw trzecich". Uściślił również, że chodzi o „system uzupełniający w stosunku do głównego systemu, ustanowionego w rozdziale II wyżej wymienionej dyrektywy, dotyczącego legalności przetwarzania danych osobowych" [47].

88. Specyfika zasad regulujących przekazywanie danych osobowych do państw trzecich w dużej mierze wynika z kluczowej roli, jaką odgrywa pojęcie odpowiedniej ochrony. W celu ustalenia zakresu tego pojęcia należy je wyraźnie odróżnić od pojęcia ochrony równoważnej, która z kolei wymaga, by państwo trzecie uznało i stosowało skutecznie wszystkie zasady zawarte w dyrektywie 95/46.

89. Pojęcie odpowiedniej ochrony oznacza, że państwo trzecie powinno być w stanie zagwarantować odpowiednią ochronę, zgodnie z modelem uznanym za możliwy do zaakceptowania pod względem stopnia ochrony danych osobowych. Taki system oparty na odpowiednim stopniu ochrony zapewnionym przez państwo trzecie pozostawia szeroki margines uznania państwom członkowskim i Komisji przy ocenianiu gwarancji zapewnionych przez państwo mające być odbiorcą danych. Przy ich badaniu należy się kierować art. 25 ust. 2 dyrektywy 95/46, w którym wymieniono niektóre kryteria, jakie można brać pod

47 — Wyrok z dnia 6 listopada 2003 r. w sprawie C-101/01 Lindqvist, Rec. str. I-12971, pkt 63.

uwagę dla potrzeb tej oceny [48]. W związku z tym zasada wprowadzona przez ustawodawcę wspólnotowego brzmi: „[o]dpowiedni stopień ochrony danych zapewnianej przez państwo trzecie należy oceniać w świetle wszystkich okoliczności dotyczących operacji przekazania danych lub zbioru takich operacji".

90. Jak wcześniej stwierdził Trybunał, dyrektywa 95/46 nie definiuje pojęcia „przekazywania do państwa trzeciego" [49]. Nie precyzuje zwłaszcza, czy pojęcie to obejmuje tylko aktywne działanie, poprzez które administrator danych przesyła dane osobowe do państwa trzeciego, czy też rozciąga się ono na sytuacje, kiedy to podmiot z państwa trzeciego jest upoważniony do posiadania dostępu do danych znajdujących się w państwie członkowskim. Zatem dyrektywa 95/46 milczy w kwestii sposobu, według jakiego może się odbywać przekazywanie danych do państwa trzeciego.

91. W przeciwieństwie do Parlamentu uważam, że w niniejszej sprawie dostęp do danych PNR, z którego korzysta CBP, wchodzi w zakres pojęcia „przekazywania do państwa trzeciego". W istocie determinujący dla scharakteryzowania takiego przekazywania jest moim zdaniem przepływ danych z państwa członkowskiego do państwa trzeciego, w niniejszym przypadku do Stanów Zjednoczonych [50]. W tym względzie nie ma większego znaczenia, czy transfer zostanie dokonany przez wysyłającego czy odbiorcę. W istocie jak uściśla EIOD, gdyby zakres art. 25 dyrektywy 95/46 był ograniczony do transferu wykonywanego przez wysyłającego, byłoby łatwo obejść wymogi wprowadzone w tym artykule.

92. Po przedstawieniu powyższego należy jednak podkreślić fakt, iż rozdział IV omawianej dyrektywy, w którym zawarty jest omawiany art. 25, nie jest przeznaczony do regulowania *wszystkich* operacji — bez względu na ich charakter — przekazywania danych osobowych do państw trzecich. Obejmuje on, zgodnie z brzmieniem art. 25 ust. 1 dyrektywy, tylko przekazywanie danych osobowych *„poddawanych przetwarzaniu* lub przeznaczonych *do przetwarzania* po ich przekazaniu".

93. Przypominam w związku z powyższym, że zgodnie z art. 2 lit. b) dyrektywy 95/46 przez przetwarzanie danych osobowych rozumie się „każdą operację lub zestaw operacji dokonywanych na danych osobo-

48 — Przypomnijmy, że wśród tych kryteriów znajduje się w szczególności charakter danych, a także cel i czas trwania proponowanych operacji przetwarzania danych.

49 — Wyżej wymieniony wyrok w sprawie Lindqvist, pkt 56. W tej sprawie Trybunał orzekł, że wpisanie danych osobowych na stronie internetowej nie stanowi „przekazywania do państwa trzeciego" w rozumieniu art. 25 dyrektywy 95/46, tylko z tego powodu, iż w ten sposób stają się one dostępne dla osób znajdujących się w państwie trzecim. Do takiego wniosku Trybunał doszedł wziąwszy pod uwagę z jednej strony techniczny charakter rozpatrywanych operacji, z drugiej zaś cel i strukturę rozdziału IV wyżej wymienionej dyrektywy, w którym zawarty jest art. 25.

50 — Mimo iż dane odbierane są przez specjalną jednostkę organizacyjną wewnętrznej struktury administracyjnej rzeczonego państwa trzeciego.

wych [...], jak np. gromadzenie, rejestracja [...], konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób [...]" [51].

94. Niezależnie od swej specyfiki, opierającej się — jak widzieliśmy — w dużym stopniu na pojęciu odpowiedniej ochrony, system dotyczący przekazywania danych osobowych do państw trzecich wymaga przestrzegania zasad związanych z zakresem stosowania dyrektywy 95/46, którego jest częścią [52].

95. Przekazywanie do państwa trzeciego, aby mogło podpadać pod przepisy art. 25 dyrektywy 95/46, powinno również dotyczyć danych osobowych, których przetwarzanie, czy to aktualnie wykonywane w ramach Wspólnoty, czy dopiero planowane w państwie trzecim, wchodzi w zakres stosowania dyrektywy. Jedynie pod tym warunkiem decyzja o odpowiedniej ochronie może w ważny sposób stanowić akt wykonawczy dyrektywy 95/46.

96. W tym względzie przypominam, że od strony ratione materiae wyżej wymieniona dyrektywa nie znajduje zastosowania do wszystkich operacji przetwarzania danych osobowych, które można zaliczyć do jednej z kategorii operacji określonych w art. 2 lit. b). W istocie art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 stanowi, że nie ma ona zastosowania do przetwarzania danych osobowych „w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. danych, 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*" [53].

97. Moim zdaniem wgląd do danych, wykorzystywanie przez CBP oraz udostępnianie

51 — Warto zaznaczyć, że pojęcia przetwarzania i przekazywania danych osobowych w pewnym stopniu się pokrywają. Na przykład ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie takich danych moim zdaniem mogą stanowić równocześnie operację ich przetwarzania oraz przekazywania w rozumieniu omawianej dyrektywy. W niniejszej sprawie pojęcia przekazywania i przetwarzania pokrywają się w zakresie, w jakim ustanowiony system ma w szczególności na celu udostępnienie dla CBP danych PNR. Taki stan rzeczy można moim zdaniem wyjaśnić bardzo szeroką definicją przetwarzania, która obejmuje obszerną listę operacji. Ostatecznie, przy takim założeniu, przekazywanie danych do państwa trzeciego oznacza szczególną formę przetwarzania. Na ten temat, zobacz projekt decyzji ramowej Komisji: art. 15, dotyczący „[transferu] danych do właściwych organów w krajach trzecich lub organów międzynarodowych", umieszczono w rozdziale III zatytułowanym „Szczególne formy przetwarzania".

52 — Zaznaczam tytułem przykładu, że decyzja Komisji 2000/519/WE z dnia 26 lipca 2000 r. w sprawie stwierdzenia, zgodnie z dyrektywą 95/46/WE, odpowiedniej ochrony danych osobowych na Węgrzech (Dz.U. L 215 str.4) stanowi w art. 1, że „[d]o celów określonych w art. 25 ust. 2 dyrektywy 95/46/WE Węgry są traktowane jako zapewniające odpowiedni poziom ochrony danych osobowych przekazywanych ze Wspólnoty *dla potrzeb wszystkich rodzajów działalności wchodzących w zakres stosowania wyżej wymienionej dyrektywy*" (podkreślenie moje) [tłumaczenie nieoficjalne].

53 — Podkreślenie moje. W przywołanym powyżej wyroku w sprawie Lindqvist Trybunał zaznaczył, że „[r]odzaje działalności wymienione tytułem przykładu w art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 [...] stanowią w każdym razie działalność właściwą państwom i władzom państwowym, odmienną od dziedzin działalności podmiotów indywidualnych", pkt 43).

CBP danych pasażerów lotniczych pochodzących z systemów rezerwacji przewoźników lotniczych znajdujących się na terytorium państw członkowskich stanowi przetwarzanie danych osobowych do celów działalności na rzecz bezpieczeństwa publicznego i jest związane z działalnością państwa w obszarach prawa karnego. Tego rodzaju przetwarzanie jest w konsekwencji wyłączone z rzeczowego zakresu stosowania dyrektywy 95/46.

98. Wyrażenia użyte w decyzji o odpowiedniej ochronie wskazują na cel przetwarzania, jakiemu poddawane są dane osobowe pasażerów lotniczych. Po wskazaniu, że wymogi przekazywania do CBP danych osobowych zawartych w PNR pasażerów lotniczych wynikają z ustawy uchwalonej przez Stany Zjednoczone w listopadzie 2001 r. oraz z przepisów wykonawczych przyjętych przez CBP na mocy wymienionej ustawy [54], Komisja dodaje, że celem ustawodawstwa amerykańskiego jest „wzmocnienie bezpieczeństwa" [55]. Wskazano również, że „Wspólnota zobowiązuje się w pełni wspierać Stany Zjednoczone w walce z terroryzmem w granicach wyznaczonych prawem wspólnotowym" [56].

99. Dodatkowo motyw piętnasty decyzji o odpowiedniej ochronie stanowi, że „dane zawarte w PNR będą wykorzystane wyłącznie do celów zapobiegania [...] terroryzm[owi] oraz związany[m] z nim przestępstw[om], inny[m] poważny[m] przestępstw[om], włącznie z przestępczością zorganizowaną, która z zasady ma charakter transnarodowy, [i zwalczania ich], oraz unikani[u] kary aresztu lub więzienia za powyższe przestępstwa".

100. Dyrektywa 95/46, a w szczególności jej art. 25 ust. 6, nie mogą moim zdaniem stanowić właściwej podstawy dla wydania przez Komisję aktu wykonawczego takiego jak decyzja w sprawie odpowiedniego poziomu ochrony danych osobowych poddawanych przetwarzaniu, które jest wyraźnie wyłączone z jej zakresu stosowania. Wyrażenie zgody na podstawie wyżej wymienionej dyrektywy na przekazywanie takich danych skutkowałoby faktycznie rozszerzeniem okrężną drogą zakresu jej stosowania.

101. Otóż należy mieć na uwadze, że dyrektywa 95/46, przyjęta na podstawie art. 100A traktatu WE, określa zasady ochrony, które powinny obowiązywać przy przetwarzaniu danych osobowych, kiedy działalność administratora danych wchodzi w zakres stosowania prawa wspólnotowego, ale z racji samego wyboru jej podstawy prawnej nie jest ona w stanie regulować tych rodzajów działalności państwa, które dotyczą bezpieczeństwa publicznego lub służą do celów

54 — Motyw szósty.
55 — Motyw siódmy.
56 — Motyw ósmy.

zwalczania przestępczości i które nie wchodzą w zakres stosowania prawa wspólnotowego [57].

102. Prawdą jest, że operacja przetwarzania, jaką stanowi gromadzenie i rejestrowanie danych pasażerów lotniczych przez przedsiębiorstwa lotnicze, ma generalnie cel gospodarczy, ponieważ jest bezpośrednio związana z przebiegiem lotu obsługiwanego przez przewoźnika lotniczego. Dlatego słusznie uważa się, że dane PNR początkowo są gromadzone przez przedsiębiorstwa lotnicze w ramach działalności podlegającej prawu wspólnotowemu, to znaczy sprzedaży biletów lotniczych uprawniających do korzystania z usług. Jednakże przetwarzanie danych unormowane w decyzji o odpowiedniej ochronie ma zupełnie odmienny charakter, jako że obejmuje etap późniejszy od początkowego gromadzenia danych. Faktycznie bowiem obejmuje — jak już widzieliśmy — wgląd do danych, wykorzystywanie przez CBP oraz udostępnianie CBP danych pasażerów lotniczych pochodzących z systemów rezerwacji przewoźników lotniczych znajdujących się na terytorium państw członkowskich.

103. W rzeczywistości decyzja o odpowiedniej ochronie nie dotyczy przetwarzania danych koniecznego w celu świadczenia usług, lecz uznanego za niezbędne dla ochrony bezpieczeństwa publicznego oraz w celach represyjnych. Taki właśnie jest cel przekazywania i przetwarzania, jakim poddawane są dane PNR. W konsekwencji fakt, iż dane osobowe zostały zgromadzone w trakcie wykonywania działalności gospodarczej. nie może moim zdaniem uzasadniać zastosowania dyrektywy 95/46, a w szczególności jej art. 25, w dziedzinie wyłączonej z zakresu jej stosowania.

104. Te przesłanki są — według mojej opinii — wystarczające, aby uznać, podobnie jak Parlament, że Komisja nie była uprawniona, na mocy art. 25 dyrektywy 95/46, do wydania decyzji dotyczącej odpowiedniej ochrony danych osobowych przekazywanych *w ramach* oraz *w celu* przetworzenia wyraźnie wyłączonego z zakresu stosowania omawianej dyrektywy [58].

57 — Zobacz artykuł na ten temat: Y. Poullet, M.V. Peres Asinan, „Données des voyageurs aériens: le débat Europe–Etats-Unis", JTDE, 2004, nr 113, str. 274. Według jego autorów „instrument, który ureguluje prawnie ten bardzo szczególny rodzaj transgranicznego przepływu powinien gwarantować prawidłowość transferu danych do zagranicznych organów administracji publicznej dokonanego w celu zwalczania terroryzmu [...] co wykracza w sposób oczywisty poza zakres stosowania dyrektywy pierwszego filaru". Dodają też, że „[t]o odpowiada, na szczeblu europejskim, jednej z dziedzin trzeciego filaru, co z kolei podważa kompetencję Komisji do działania w tym zakresie [...]". Zobacz także O. De Schutter, „La Convention européenne des droits de l'homme à l'épreuve de la lutte contre le terrorisme", w: „Lutte contre le terrorisme et droits fondamentaux", E. Bribosia, A. Weyembergh (dir.), „Collection droit et justice", Bruylant, Bruksela 2002, str. 112, nota nr 43: po przytoczeniu art. 3 ust. 2 tiret pierwsze dyrektywy 95/46, autor zauważa, że „[t]o ograniczenie zakresu stosowania [d]yrektywy tłumaczy się ograniczonym zakresem kompetencji Wspólnoty Europejskiej, która nie ma kompetencji ogólnej do stanowienia prawa w dziedzinie praw człowieka, ale może działać w tej dziedzinie w szczególności na obszarze oraz w stopniu, w jakim — jak w przypadku [wyżej wymienionej dyrektywy] — chodzi o ułatwienie tworzenia rynku wewnętrznego, które wymaga usunięcia przeszkód dla swobodnego przepływu towarów i swobody świadczenia usług".

58 — Dane PNR są poddawane przetwarzaniu wewnątrz Wspólnoty, polegającemu na ich udostępnieniu CBP. Równocześnie są przeznaczone do przetwarzania po przekazaniu, z racji ich wykorzystania przez CBP.

105. Zatem decyzja o odpowiedniej ochronie stanowi naruszenie aktu podstawowego, jakim jest dyrektywa 95/46, a w szczególności jej art. 25, który nie jest właściwą podstawą prawną dla decyzji. Uważam, że z tego względu należy stwierdzić jej nieważność.

106. Ponadto ponieważ stoję na stanowisku, że decyzja o odpowiedniej ochronie wykracza poza zakres stosowania dyrektywy 95/46, nie wydaje mi się zasadne analizowanie — o co wnosi Parlament w swoim zarzucie drugim — tej decyzji pod kątem podstawowych zasad zawartych w wyżej wymienionej dyrektywie[59]. Uważam więc, że nie ma potrzeby badania zarzutu drugiego.

107. Co do zarzutów trzeciego i czwartego podniesionych w omawianej skardze, które rozważę jedynie tytułem ewentualnym, moim zdaniem nie mogą one być oddzielnie analizowane, ponieważ badanie naruszenia praw podstawowych przez decyzję o odpowiedniej ochronie musi obejmować ocenę przestrzegania zasady proporcjonalności przez ten akt prawny w świetle celu, którego osiągnięciu służy. Proponuję zatem Trybunałowi, aby zarzuty trzeci i czwarty zbadał równocześnie.

B — *W przedmiocie zarzutów opartych na naruszeniu praw podstawowych oraz naruszeniu zasady proporcjonalności*

108. Parlament utrzymuje, że decyzja o odpowiedniej ochronie nie respektuje prawa do ochrony danych osobowych, które gwarantuje art. 8 EKPC. Dokładniej rzecz ujmując, Parlament uważa, że w świetle zasad określonych w tym artykule omawiana decyzja stanowi ingerencję w życie prywatne, której nie można uznać za przewidzianą przez ustawę, ponieważ mamy do czynienia ze środkiem, który nie jest ani dostępny, ani przewidywalny. Ponadto Parlament stoi na stanowisku, że ten środek nie jest proporcjonalny do celu, do jakiego służy, zwłaszcza wziąwszy pod uwagę przesadnie dużą liczbę żądanych elementów danych PNR oraz nadmiernie długi okres przechowywania danych.

109. W skardze wniesionej w sprawie C-317/04 o stwierdzenie nieważności decyzji Rady Parlament również podnosi te dwa zarzuty, a na ich poparcie przedstawia argumenty, które w dużej części się pokrywają. Uważam, że te zarzuty, zgłoszone

59 — Co nie oznacza, by decyzja o odpowiedniej ochronie wydana w sytuacji podobnej do zaistniałej w niniejszej sprawie powinna być uważana w porządku prawnym Unii Europejskiej za zwolnioną z obowiązku zapewnienia podstawowych gwarancji w dziedzinie ochrony danych osobowych, w szczególności wymienionych w konwencji nr 108. Tyle że w tych okolicznościach uważam, iż dyrektywa 95/46 nie jest odpowiednim aktem podstawowym, w przypadku gdy — jak widzieliśmy — cele decyzji o odpowiedniej ochronie wykraczają poza zakres stosowania normy podstawowej, jaką stanowi omawiana dyrektywa. W związku z tym wobec braku normy prawa pochodnego mającej zastosowanie do przetwarzania danych osobowych do celów zwalczania przestępczości oraz bezpieczeństwa publicznego nie jest możliwe, by przystąpić do abstrakcyjnej kontroli sądowej wspomnianych wyżej gwarancji. Ochrona sądowa jednak istnieje również i w takiej sytuacji. W istocie kontrola podstawowych gwarancji w dziedzinie ochrony danych osobowych jest — jak zobaczymy — ściśle związana z badaniem wymogów określonych w art. 8 ust. 2 EKPCz.

w obydwu sprawach wniesionych do Trybunału, powinny zostać zbadane równocześnie i uznałem za słuszne, by zrobić to przy okazji analizowania sprawy C-317/04.

110. Z argumentów podniesionych przez strony w pismach procesowych wynika faktycznie, iż nie można, w świetle prawa do poszanowania życia prywatnego, rozpatrywać oddzielnie elementów systemu związanego z przetwarzaniem danych PNR przez CBP [60], na który to system składają się porozumienie zatwierdzone decyzją Rady, decyzja o odpowiedniej ochronie oraz Zobowiązania CBP załączone do wspomnianej decyzji Komisji. Strony odsyłają zresztą wielokrotnie do jednego lub drugiego z tych aktów w celu poparcia swoich twierdzeń.

111. Wzajemne zależności pomiędzy tymi trzema elementami składowymi systemu PNR wynikają jasno z samego brzmienia porozumienia. Zarówno Zobowiązania CBP, jak i decyzja o odpowiedniej ochronie, są bowiem wymienione w preambule porozumienia. Następnie pkt 1 porozumienia precyzuje, że CBP może posiadać dostęp do danych PNR „w ścisłej zgodności z decyzją [o odpowiedniej ochronie] i tak długo dopóki decyzja ma zastosowanie [...]". Na podobnej zasadzie pkt 2 porozumienia przewiduje, że wprawdzie wskazani w nim przewoźnicy muszą przetwarzać dane PNR „zgodnie z wymaganiami Biura Ceł i Ochrony Granic (CBP) odpowiednio do prawa Stanów Zjednoczonych", jednak nadal „w ścisłej zgodności z decyzją [o odpowiedniej ochronie] i tak długo dopóki decyzja ma zastosowanie". Wreszcie pkt 3 porozumienia stanowi, że „Biuro Ceł i Ochrony Granic (CBP) przyjmuje do wiadomości decyzję [o odpowiedniej ochronie] i stwierdza, że wprowadza w życie zobowiązania załączone do niej".

112. Z przytoczonych postanowień wynika, że prawo dostępu do danych PNR przyznane CBP przez porozumienie, a także obowiązek przetwarzania przedmiotowych danych nałożony na przewoźników lotniczych wskazanych w porozumieniu, są uzależnione od ścisłego i faktycznego stosowania decyzji o odpowiedniej ochronie.

113. Wzajemne zależności pomiędzy trzema elementami systemu PNR, a także fakt, iż zarzuty naruszenia praw podstawowych i zasady proporcjonalności zostały podniesione przez Parlament w obydwu sprawach wniesionych do rozstrzygnięcia przez Trybunał, prowadzą do wniosku, że zarzuty te należy rozumieć w ten sposób, że mają one na celu stwierdzenie przez Trybunał niezgodności systemu PNR w tych trzech elementach, z prawem do poszanowania życia prywatnego zagwarantowanym przez art. 8 EKPC. Moim zdaniem byłoby raczej rzeczą nienaturalną badanie decyzji o odpowiedniej ochronie bez uwzględnienia porozumienia, które nakłada na przedsiębiorstwa lotnicze określone obowiązki, a także w drugą stronę — badanie porozumienia bez brania pod uwagę innych obowiązujących aktów prawnych, do których porozumienie wyraźnie nawiązuje.

60 — Zwanego dalej „systemem PNR".

114. Zważywszy, iż system składa się z kilku nierozłącznych elementów, analiza nie powinna więc być podzielona w sposób sztuczny.

115. Ingerencję w życie prywatne, rozpatrywaną pod tym kątem, stanowi pakiet aktów, na który składa się porozumienie zatwierdzone decyzją Rady, decyzja o odpowiedniej ochronie oraz Zobowiązania CBP. W celu zbadania, czy ingerencja ta była przewidziana ustawą, jej cel był uprawniony i czy była konieczna w demokratycznym społeczeństwie, trzeba również wziąć pod uwagę cały mechanizm „trójbiegowy" stworzony w ten sposób, tak jak to czyni Parlament w swoich dwóch skargach. Aby mieć widok ogólny na system PNR, przystąpię do jego badania w ramach skargi o stwierdzenie nieważności decyzji Rady.

VI — W przedmiocie skargi o stwierdzenie nieważności decyzji Rady (sprawa C-317/04)

A — *W przedmiocie zarzutu błędnego wyboru art. 95 WE jako podstawy prawnej decyzji Rady*

1. Argumenty stron

116. Parlament Europejski twierdzi, że art. 95 WE nie stanowi podstawy prawnej właściwej dla decyzji Rady. Jej celem ani treścią nie jest bowiem ustanowienie lub funkcjonowanie rynku wewnętrznego. Celem decyzji Rady jest raczej legalizacja przetwarzania danych osobowych wymaganego przez amerykańskie ustawodawstwo od przedsiębiorstw lotniczych działających na obszarze Wspólnoty. Decyzja nie określa, w jakim zakresie legalizacja transferu danych do państwa trzeciego miałby się przyczyniać do ustanowienia lub funkcjonowania wspólnego rynku.

117. Zdaniem Parlamentu treść decyzji Rady nie uzasadnia również zastosowania art. 95 WE jako podstawy prawnej. Decyzja ta zasadza się bowiem na ustanowieniu prawa dostępu dla CBP do systemów rezerwacji przedsiębiorstw lotniczych na terytorium Wspólnoty, w związku z realizowaniem lotów pomiędzy Stanami Zjednoczonymi a państwami członkowskimi, zgodnie z ustawodawstwem amerykańskim, w celu zapobiegania i zwalczania terroryzmu. Tymczasem realizacja tych celów nie podpada pod art. 95 WE.

118. Na koniec Parlament dodaje, że art. 95 WE nie mógłby stanowić podstawy kompetencji Wspólnoty do zawarcia porozumienia, ponieważ dotyczy ono przetwarzania danych do celów związanych z bezpieczeństwem publicznym, a zatem wyłączo-

nych z zakresu stosowania dyrektywy 95/46 opartej na wyżej wymienionym artykule traktatu.

119. Natomiast Rada stoi na stanowisku, że jej decyzja została prawidłowo wydana na podstawie art. 95 WE. Według niej artykuł ten może uzasadniać środki służące zapewnieniu, by warunki konkurencji na rynku wewnętrznym nie zostały zakłócone. Utrzymuje ona w tym względzie, że porozumienie ma na celu wyeliminowanie wszelkich zakłóceń konkurencji między przedsiębiorstwami lotniczymi z państw członkowskich oraz między nimi a przedsiębiorstwami lotniczymi z państw trzecich, jakie mogłyby wyniknąć, ze względu na ochronę praw i wolności człowieka, z wymogów nałożonych przez Stany Zjednoczone. Warunki konkurencji między przedsiębiorstwami lotniczymi z państw członkowskich świadczącymi usługi międzynarodowego przewozu pasażerów do i ze Stanów Zjednoczonych mogłyby zostać zakłócone z tego powodu, że tylko niektóre z nich udostępniły władzom Stanów Zjednoczonych swoje bazy danych.

120. Idąc dalej tym tokiem rozumowania Rada podkreśla, że z jednej strony przedsiębiorstwa lotnicze, które nie spełniłyby amerykańskich wymogów, byłyby narażone na kary pieniężne nakładane przez władze amerykańskie, na opóźnienia swoich lotów oraz utratę pasażerów na rzecz innych linii lotniczych, które zawarły porozumienie ze Stanami Zjednoczonymi, z drugiej strony niektóre państwa członkowskie mogłyby nakładać kary na przedsiębiorstwa lotnicze przekazujące dane osobowe, o których mowa, podczas gdy inne państwa członkowskie niekoniecznie musiałyby postępować w ten sposób.

121. W tych okolicznościach przy braku wspólnych regulacji dotyczących dostępu dla władz amerykańskich do danych PNR Rada uważa, że istniało ryzyko zakłócenia warunków konkurencji i mogłoby dojść do poważnego naruszenia jedności rynku wewnętrznego. Zatem jej zdaniem konieczne było wprowadzenie jednolitych zasad regulujących dostęp władz amerykańskich do tych danych z zachowaniem wymogów wspólnotowych pod względem poszanowania praw podstawowych. Chodziło o nałożenie na wszystkie przedsiębiorstwa lotnicze jednakowych obowiązków oraz o zewnętrzne aspekty ustanawiania i funkcjonowania rynku wewnętrznego.

122. Na koniec Rada zaznacza, że porozumienie zostało zawarte po wydaniu decyzji o odpowiedniej ochronie, przyjętej na mocy art. 25 ust. 6 dyrektywy 95/46. Według niej, było więc normalne i prawidłowe, że oparto decyzję w sprawie zawarcia porozumienia na tej samej podstawie prawnej, jaką zastosowano do wyżej wymienionej dyrektywy, tj. na art. 95 WE.

123. W swoich uwagach interwenienta Komisja podkreśla, że postanowienia preambuły porozumienia wskazują, iż dla Stanów Zjednoczonych priorytetowym celem jest walka z terroryzmem, natomiast dla Wspólnoty główny cel to zachowanie zasadniczych elementów swojego ustawodawstwa w zakresie ochrony danych osobowych.

125. Na koniec Komisja podniosła argument, że początkowe przetwarzanie tych danych przez przedsiębiorstwa lotnicze następuje dla celów działalności gospodarczej. Zatem użytek, jaki z tych danych czynią władze Stanów Zjednoczonych, nie powoduje ich wyłączenia spod działania dyrektywy 95/46.

2. Ocena

124. Komisja zwraca uwagę, że krytykując wybór art. 95 WE jako podstawy prawnej decyzji Rady, Parlament nie przedstawił rozwiązania alternatywnego niebudzącego wątpliwości. Według Komisji ten artykuł stanowi „naturalną" podstawę prawną dla decyzji Rady, gdyż zewnętrzny wymiar ochrony danych osobowych powinien opierać się na artykule traktatu, który stanowi podstawę środka wewnętrznego, jakim jest dyrektywa 95/46, tym bardziej że te aspekty zewnętrzne zostały wyraźnie przewidziane w art. 25 i 26 wyżej wymienionej dyrektywy. Ponadto z uwagi na ścisły związek i wzajemne zależności pomiędzy porozumieniem, decyzją o odpowiedniej ochronie i Zobowiązaniami CBP art. 95 WE okazuje się być właściwą podstawą prawną. W każdym razie Komisja utrzymuje, że Rada miała kompetencję do zawarcia porozumienia na podstawie tego artykułu, ponieważ doszłoby do naruszenia dyrektywy 95/46, w rozumieniu orzecznictwa AETR [61], gdyby państwa członkowskie zawarły takie porozumienie, razem lub każde z osobna, poza ramami wspólnotowymi.

126. Zgłaszając swój zarzut pierwszy Parlament zwraca się do Trybunału o rozstrzygnięcie, czy art. 95 WE stanowi podstawę prawną dla decyzji Rady w sprawie zawarcia przez Wspólnotę porozumienia międzynarodowego takiego rodzaju, jak będące przedmiotem niniejszej sprawy. Aby odpowiedzieć na to pytanie, należy odwołać się do utrwalonego orzecznictwa Trybunału, zgodnie z którym wybór podstawy prawnej aktu wspólnotowego powinien opierać się na obiektywnych przesłankach podlegających kontroli sądowej, do których zalicza się między innymi cel i treść aktu [62]. W istocie „w ramach organizacji kompetencji we Wspólnocie wybór podstawy prawnej aktu

61 — Wyrok z dnia 31 marca 1971 r. w sprawie 22/70 Komisja przeciwko Radzie, zwanej „AETR", Rec. str. 263.

62 — Zobacz m.in. wyroki: z dnia 11 czerwca 1991 r. w sprawie C-300/89 Komisja przeciwko Radzie, zwanej „Dwutlenek tytanu", Rec. str. I-2867, pkt 10; z dnia 12 listopada 1996 r. w sprawie C-84/94 Zjednoczone Królestwo przeciwko Radzie, Rec. str. I-5755, pkt 25; z dnia 25 lutego 1999 r. w sprawach połączonych C-164/97 i C-165/97 Parlament przeciwko Radzie, Rec. str. I-1139, pkt 12; z dnia 4 kwietnia 2000 r. w sprawie C-269/97 Komisja przeciwko Radzie, Rec. str. I-2257, pkt 43; z dnia 19 września 2002 r. w sprawie C-336/00 Huber, Rec. str. I-7699, pkt 30; z dnia 29 kwietnia 2004 r. w sprawie C-338/01 Komisja przeciwko Radzie, Rec. str. I-4829, pkt 54, oraz z dnia 13 września 2005 r. w sprawie C-176/03 Komisja przeciwko Radzie, Zb.Orz. str. I-7879, pkt 45).

nie może zależeć tylko od przeświadczenia instytucji co do celu, któremu ma on służyć [...]" [63].

127. Przypominam, że Trybunał orzekł, że „wybór właściwej podstawy prawnej ma znaczenie o charakterze konstytucyjnym. Ponieważ Wspólnota posiada tylko kompetencje nadane, musi powiązać [daną umowę międzynarodową] z postanowieniem traktatu, które ją upoważnia do zatwierdzenia takiego aktu". Według Trybunału „[b]łędne powołanie podstawy prawnej może więc spowodować nieważność samej czynności zawarcia umowy, a w związku z tym wadę oświadczenia woli dotyczącego zgody Wspólnoty na związanie się umową, którą podpisała" [64].

128. Posługując się metodą analizy stosowaną przez Trybunał, zbadam więc, czy cel oraz treść porozumienia upoważniały Radę do przyjęcia na podstawie art. 95 WE decyzji, której przedmiotem, zgodnie z brzmieniem jej art. 1, jest zatwierdzenie w imieniu Wspólnoty rzeczonego porozumienia.

129. Jeśli chodzi o cel porozumienia, z akapitu pierwszego jego preambuły wynika wyraźnie, że służy ono dwóm celom: z jednej strony zapobieganiu terroryzmowi oraz związanym z nim przestępstwom, a także innym poważnym przestępstwom o ponadnarodowym charakterze, włącznie z przestępczością zorganizowaną, i zwalczaniu ich [65], z drugiej zaś strony poszanowaniu podstawowych praw i wolności, a w szczególności prawa do prywatności.

130. O dążeniu do celu zwalczania terroryzmu i innych poważnych przestępstw świadczy wzmianka w akapicie drugim preambuły porozumienia o wydanych w następstwie ataków terrorystycznych z dnia 11 września 2001 r. amerykańskich ustawach i rozporządzeniach, które wymagają od każdego przewoźnika lotniczego świadczącego usługi międzynarodowego przewozu pasażerów do i ze Stanów Zjednoczonych zapewnienia elektronicznego dostępu dla CBP do danych PNR gromadzonych i przechowywanych w jego automatycznym systemie kontroli rezerwacji i odlotów.

131. Co się zaś tyczy celu związanego z poszanowaniem podstawowych praw i wolności, a w szczególności prawa do prywatności, pojawia się on poprzez nawiązanie do dyrektywy 95/46. Chodzi o zagwarantowanie podróżującym osobom fizycznym ochrony ich danych osobowych.

63 — Wyrok z dnia 26 marca 1987 r. w sprawie 45/86 Komisja przeciwko Radzie, Rec. str. 1493, pkt 11.

64 — Opinia 2/00 z dnia 6 grudnia 2001 r. wydana na podstawie art. 300 ust. 6 WE, Rec. str. I-9713, pkt 5.

65 — W dalszej części wywodów dla określenia tego celu będę używał wyrażenia „zwalczanie terroryzmu i innych poważnych przestępstw".

132. Tej gwarancji poszukuje się zarówno w zobowiązaniach podjętych przez CBP w dniu 11 maja 2004 r., na temat których w akapicie czwartym preambuły porozumienia stwierdza się, że zostaną opublikowane w *Federal Register*, jak i w decyzji o odpowiedniej ochronie, o której jest mowa w akapicie piątym preambuły.

133. Obydwa cele powinny, zgodnie z akapitem pierwszym preambuły porozumienia, być realizowane równocześnie. Porozumienie zawarte pomiędzy Wspólnotą a Stanami Zjednoczonymi stara się zatem pogodzić te dwa cele, to oznacza, że opiera się na idei prowadzenia walki z terroryzmem i innymi poważnymi przestępstwami z poszanowaniem praw podstawowych oraz w szczególności prawa do prywatności, a dokładniej prawa do ochrony danych osobowych.

134. Treść porozumienia potwierdza tę analizę. W pkt 1 przewidziano bowiem, że CBP może mieć dostęp drogą elektroniczną do danych PNR pochodzących z systemów kontroli rezerwacji przewoźników lotniczych znajdujących się na terytorium państw członkowskich „w ścisłej zgodności" z decyzją o odpowiedniej ochronie „i tak długo [jak długo] decyzja ma zastosowanie". Na tej podstawie dochodzę do przekonania, że środek służący zwalczaniu terroryzmu oraz innych poważnych przestępstw, jaki stanowi dostęp do danych PNR pasażerów lotniczych, jest dozwolony przez porozumienie tylko pod warunkiem, że zostanie stwierdzone, że dane te mają zapewniony w Stanach Zjednoczonych odpowiedni poziom ochrony. Treść tego postanowienia porozumienia wyraża więc dążenie równocześnie do zwalczania terroryzmu i innych poważnych przestępstw oraz do ochrony danych osobowych.

135. Taki sam wniosek narzuca się przy badaniu pkt 2 porozumienia, który nakłada na przewoźników lotniczych świadczących usługi międzynarodowego przewozu pasażerów do i ze Stanów Zjednoczonych obowiązek przetwarzania danych PNR zawartych w ich informatycznych systemach rezerwacji, „zgodnie z wymaganiami Biura Ceł i Ochrony Granic (CBP) odpowiednio do prawa Stanów Zjednoczonych i w ścisłej zgodności z decyzją [o odpowiedniej ochronie] oraz tak długo [jak długo] decyzja ma zastosowanie". Tu również obowiązek spoczywający odtąd na przewoźnikach lotniczych dla potrzeb zwalczania terroryzmu i innych poważnych przestępstw jest ściśle związany z ochroną danych osobowych pasażerów lotniczych.

136. Inne postanowienia porozumienia mają odzwierciedlać cele w postaci zwalczania terroryzmu i innych poważnych przestępstw

oraz ochrony danych osobowych pasażerów lotniczych.

137. Na przykład w kwestii samego celu ochrony danych osobowych pasażerów w pkt 3 porozumienia wskazano, że „Biuro Ceł i Ochrony Granic (CBP) przyjmuje do wiadomości decyzję [o odpowiedniej ochronie] i stwierdza, że wprowadza w życie zobowiązania załączone do niej".

138. Ponadto pkt 6 porozumienia przewiduje sytuację, że z kolei Unia Europejska wprowadziłaby system identyfikacji pasażerów lotniczych, w ramach którego wymagałaby od przewoźników lotniczych udostępnienia właściwym władzom danych PNR pasażerów na trasach obejmujących przelot do lub z Unii Europejskiej. W takim przypadku Department of Homeland Security „jeśli tylko ma to zastosowanie i ściśle w oparciu o zasadę wzajemności, aktywnie promuje współpracę linii lotniczych w ramach swojej właściwości". Mamy tu do czynienia z kolejnym postanowieniem, które wiąże się z celem zwalczania terroryzmu i innych poważnych przestępstw.

139. Uściślam w tym względzie — w odpowiedzi na niektóre argumenty Komisji — że moim zdaniem trudno utrzymywać, iż do realizacji celu zwalczania terroryzmu i innych poważnych przestępstw dążyły jednostronnie tylko Stany Zjednoczone, a Wspólnota miała na celu wyłącznie ochronę danych osobowych pasażerów lotniczych [66]. Uważam, że celem i treścią porozumienia, z punktu widzenia każdej z umawiających się stron równocześnie, było pogodzenie zwalczania terroryzmu i innych poważnych przestępstw z ochroną danych osobowych pasażerów lotniczych. W związku z tym porozumienie ustanawia współpracę pomiędzy umawiającymi się stronami, która ma dokładnie za zadanie realizować obydwa cele jednocześnie.

140. W świetle tak przedstawionych celu i treści porozumienia uważam, że art. 95 WE nie stanowi właściwej podstawy prawnej dla decyzji Rady.

141. Należy w tym miejscu przypomnieć, że art. 95 ust. 1 WE odnosi się do przyjmowania przez Radę środków dotyczących zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego.

66 — Poza tym terroryzm jest zjawiskiem międzynarodowym, które drwi sobie z podziałów terytorialnych.

142. Kompetencja powierzona Wspólnocie na mocy tego artykułu traktatu ma charakter horyzontalny, tzn. nie jest ograniczona do jednej określonej dziedziny. Zakres kompetencji wspólnotowej jest więc określony „według kryterium *funkcjonalnego*, rozciągając się poziomo na wszystkie środki przeznaczone do realizacji »rynku wewnętrznego«" [67].

143. Ponadto z orzecznictwa Trybunału wynika, że środki, o których mowa w art. 95 ust. 1 WE, są przeznaczone do poprawienia warunków tworzenia i funkcjonowania rynku wewnętrznego i powinny faktycznie mieć taki cel, przyczyniając się do zniesienia przeszkód dla swobodnego przepływu towarów lub swobody świadczenia usług lub do zlikwidowania zakłóceń konkurencji [68]. Z tego orzecznictwa wypływa również wniosek, że art. 95 WE może zostać przyjęty za podstawę prawną w celu zapobieżenia przyszłym przeszkodom w wymianie handlowej wynikającym z niejednolitego rozwoju krajowych przepisów prawnych, jednakże wystąpienie takich przeszkód musi być prawdopodobne, zaś zamierzony środek musi mieć na celu zapobieżenie im [69].

144. Jak już mówiłem, Rada utrzymuje, że jej decyzja została wydana ważnie na podstawie art. 95 WE, ponieważ eliminując wszelkie zakłócenia konkurencji między przedsiębiorstwami lotniczymi z państw członkowskich oraz między nimi a przedsiębiorstwami lotniczymi z państw trzecich, porozumienie ze Stanami Zjednoczonymi przyczyniło się do zapobieżenia poważnemu naruszeniu jedności rynku wewnętrznego.

145. Należy zauważyć, iż rzeczywiście motyw drugi decyzji Rady nawiązuje do „piln[ej] potrzeb[y] zapobieżenia sytuacji niepewności, w której znajdują się linie lotnicze i pasażerowie, i ochrony interesów finansowych zainteresowanych podmiotów". To zdanie można by rozumieć jako nawiązujące do sankcji, jakie mogą być nałożone przez właściwe władze amerykańskie na przedsiębiorstwa lotnicze, które odmówiłyby udostępnienia danych PNR swoich pasażerów, sankcji, które mogłyby mieć dla tych przedsiębiorstw konsekwencje finansowe. Można by zatem założyć, że w takim przypadku sankcje pociągające za sobą niekorzystne skutki finansowe dla niektórych przedsiębiorstw lotniczych mogłyby być

67 — Zobacz pkt 10 opinii rzecznika generalnego G. Tesaura w ww. sprawie „Dwutlenek węgla".

68 — Wyroki z dnia 5 października 2000 r. w sprawie C-376/98 Niemcy przeciwko Parlamentowi i Radzie, Rec. str. I-8419, pkt 83, 84 i 95, oraz z dnia 10 grudnia 2002 r. w sprawie C-491/01 British American Tobacco (Investments) i Imperial Tobacco, Rec. str. I-11453, pkt 60.

69 — Zobacz podobnie wyrok z dnia 13 lipca 1995 r. w sprawie C-350/92 Hiszpania przeciwko Radzie, Rec. str. I-1985, pkt 35, a także ww. wyrok w sprawie Niemcy przeciwko Parlamentowi i Radzie, pkt 86; wyrok z dnia 9 października 2001 r. w sprawie C-377/98 Niderlandy przeciwko Parlamentowi i Radzie, Rec. str. I-7079, pkt 15; ww. wyrok w sprawie British American Tobacco (Investments) i Imperial Tobacco, pkt 61, oraz wyrok z dnia 14 grudnia 2004 r. w sprawie C-434/02 Arnold André, Zb.Orz. str. I-11825, pkt 31.

przyczyną zakłócenia konkurencji pomiędzy wszystkimi przedsiębiorstwami lotniczymi, które ustanowiły działalność na terytorium państw członkowskich.

146. Co więcej, można także założyć ewentualność, że fakt, iż państwa członkowskie przyjęłyby różne postawy, jedne pod groźbą kary zakazałyby przedsiębiorstwom lotniczym prowadzącym działalność na ich terytorium zezwalać na transfer danych PNR swoich pasażerów, podczas gdy inne zachowałyby się w sposób zgoła odmienny, mógłby mieć wpływ, choćby pośredni, na funkcjonowanie rynku wewnętrznego ze względu na ewentualne zakłócenia konkurencji między przedsiębiorstwami lotniczymi, jakie mogłyby powstać.

147. Jednakże należy stwierdzić, że taki cel, związany z zapobieganiem zakłóceniom konkurencji — przy założeniu, że Rada rzeczywiście do niego dążyła — ma *charakter dodatkowy w* stosunku do dwóch głównych celów: zwalczania terroryzmu i innych poważnych przestępstw oraz ochrony danych osobowych pasażerów, które to — jak widzieliśmy — zostały wyraźnie wymienione i faktycznie wdrożone postanowieniami porozumienia.

148. Cel związany z zapobieganiem zakłóceniom konkurencji, czy to — jak twierdzi Rada — między przedsiębiorstwami lotniczymi z państw członkowskich, czy między nimi a przedsiębiorstwami lotniczymi z państw trzecich, nigdzie nie został wyraźnie jako taki wymieniony w postanowieniach porozumienia. Ma on charakter dorozumiany, a zatem musi być dodatkowy w stosunku do dwóch pozostałych.

149. Przypominam, że — jak już wcześniej orzekł Trybunał — „sam fakt, iż akt może mieć wpływ na tworzenie i funkcjonowanie rynku wewnętrznego, nie jest wystarczający, by uzasadnić zastosowanie tego postanowienia jako podstawy prawnej tego aktu" [70].

150. Przede wszystkim zaś z utrwalonego orzecznictwa Trybunału wynika, że jeśli analiza aktu wspólnotowego wykazuje, że służy on kilku celom lub składa się z kilku elementów, i jeśli jeden z nich można wskazać jako główny lub przeważający, podczas gdy drugi jest jedynie dodatkowym, taki akt powinien opierać się tylko na jednej podstawie prawnej, tj. tej wymaganej ze względu na cel lub element główny lub przeważający [71]. Tylko w wyjątkowych przypadkach, jeśli wykazano, że akt służy równocześnie kilku celom powiązanym ze sobą w sposób nierozdzielny, tak że żaden nie jest wtórny czy pośredni w stosunku do drugiego,

70 — Zobacz w szczególności wyrok z dnia 9 listopada 1995 r. w sprawie C-426/93 Niemcy przeciwko Radzie, Rec. str. I-3723, pkt 33.

71 — Zobacz w szczególności wyroki: z dnia 17 marca 1993 r. w sprawie C-155/91 Komisja przeciwko Radzie, Rec. str. I-939, pkt 19 i 21; z dnia 23 lutego 1999 r. w sprawie C-42/97 Parlament przeciwko Radzie, Rec. str. I-869, pkt 39 i 40; z dnia 30 stycznia 2001 r. w sprawie C-36/98 Hiszpania przeciwko Radzie, Rec. str. I-779, pkt 59, oraz z dnia 12 grudnia 2002 r. w sprawie C-281/01 Komisja przeciwko Radzie, Rec. str. I-12049, pkt 34.

taki akt powinien być oparty na różnych podstawach prawnych odpowiadających poszczególnym celom [72]. Moim zdaniem w rozpoznawanej sprawie taka sytuacja nie występuje.

151. Chcę jeszcze podkreślić, że nawet jeśli wszystkie trzy cele miałyby być uważane za realizowane przez porozumienie w sposób nierozłączny, nie zmienia to faktu, iż wybór Rady co do oparcia decyzji na samym tylko art. 95 WE jako podstawie prawnej powinien w świetle tego orzecznictwa zostać uznany za niewłaściwy.

152. W rzeczywistości z lektury motywu drugiego decyzji Rady w pełnym brzmieniu wynika, że „pilna potrzeba", o której w nim mowa, wiąże się z wyjaśnieniem, że Parlamentowi wyznaczono termin na przedstawienie opinii, zgodnie z art. 300 ust. 3 akapit pierwszy WE, który przewiduje, że w ramach procedury zawierania umów „Parlament Europejski wyraża swoją opinię w terminie, który może ustalić Rada, stosownie do pilności sprawy". Artykuł ten stanowi również, że „[w] przypadku braku opinii w tym terminie Rada może stanowić samodzielnie". Taka sytuacja miała miejsce w trakcie procedury przeprowadzonej w celu wydania decyzji Rady.

153. Inaczej mówiąc, wprawdzie „piln[a] potrzeb[a] zapobieżenia sytuacji niepewności, w której znajdują się linie lotnicze i pasażerowie, i ochrony interesów finansowych zainteresowanych podmiotów" mogła faktycznie być brana pod uwagę w procesie tworzenia systemu dla danych PNR, wydaje mi się, że jej uwzględnienie odegrało większą rolę w ramach przeprowadzonej procedury niż w określaniu celu i treści porozumienia.

154. Co do argumentu podnoszonego przez Radę i Komisję, że akt dotyczący zewnętrznego wymiaru ochrony danych osobowych powinien być oparty na tej samej podstawie prawnej co środek wewnętrzny, tzn. dyrektywa 95/46, należy podkreślić, że Trybunał orzekł już wcześniej, że fakt, iż określone postanowienie traktatu zostało wybrane jako podstawa prawna do przyjęcia aktów wewnętrznych nie wystarczy do wykazania, że ta sama podstawa prawna powinna być również wybrana w celu zatwierdzenia umowy międzynarodowej mającej podobny przedmiot [73]. Co więcej, wykazałem, że ani głównym celem, ani treścią porozumienia nie była poprawa warunków funkcjonowania rynku wewnętrznego, podczas gdy dyrektywa 95/46, przyjęta na mocy art. 95 WE, „służy zapewnieniu swobodnego przepływu danych osobowych między państwami członkowskimi przez ujednolicenie przepisów krajowych o ochronie osób fizycznych w odnie-

72 — Zobacz w szczególności ww. wyroki: w sprawie „Dwutlenek węgla", pkt 13 i 17; z dnia 23 lutego 1999 r. w sprawie Parlament przeciwko Radzie, pkt 38 i 43; Huber, pkt 31, oraz z dnia 12 grudnia 2002 r. w sprawie Komisja przeciwko Radzie, pkt 35.

73 — Wyżej wymieniony wyrok z dnia 12 grudnia 2002 r. w sprawie Komisja przeciwko Radzie, pkt 46.

sieniu do przetwarzania takich danych" [74].

155. Wziąwszy pod uwagę powyższe stwierdzenia, uważam, że badanie celu i treści porozumienia wykazuje, iż art. 95 WE nie stanowi podstawy prawnej odpowiedniej dla decyzji Rady.

156. W związku z tym proponuję Trybunałowi, by orzekł, że zarzut pierwszy zgłoszony przez Parlament jest zasadny. Wynika stąd, że należy stwierdzić nieważność decyzji Rady z powodu błędnego wyboru podstawy prawnej.

157. Byłoby z pewnością interesujące zadać w tym stadium pytanie, jaka powinna być podstawa prawna właściwa dla tego rodzaju decyzji. Należy jednak zaznaczyć, iż ta delikatna kwestia nie wchodzi w zakres orzekania Trybunału w ramach niniejszej sprawy. Przedstawię zatem tylko kilka uwag na ten temat oraz ogólnie na temat istoty systemu PNR, w postaci w jakiej został wynegocjowany ze Stanami Zjednoczonymi.

158. Przede wszystkim wbrew koncepcji bronionej przez Radę, okoliczność, iż system PNR nie został wprowadzony w ramach postanowień traktatu UE, nie jest — moim zdaniem — w stanie wykazać prawnej ważności rozwiązania zastosowanego przez Radę i Komisję.

159. Ponadto generalnie sądzę, że akt przewidujący wgląd do danych osobowych i ich wykorzystywanie przez podmiot, którego funkcja polega na zapewnieniu ochrony bezpieczeństwa wewnętrznego państwa, a także udostępnianie tych danych takiemu podmiotowi, można traktować na równi z aktem współpracy pomiędzy władzami publicznymi [75].

160. Co więcej, nie wydaje się, by wymaganie od osoby prawnej takiego przetwarzania danych i obligowanie jej do dokonania transferu danych zasadniczo różniło się od bezpośredniej wymiany danych pomiędzy

74 — Wyrok z dnia 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 Österreichischer Rundfunk i in., Rec. str. I-4989, pkt 39). Zważywszy na odmienność przedmiotu i celu porozumienia i dyrektywy 95/46, sądzę również, iż jest nieprawdopodobne, by — jak utrzymuje Komisja — doszło do naruszenia dyrektywy w rozumieniu orzecznictwa AETR, gdyby państwa członkowskie, każde oddzielnie lub razem, zawarły porozumienie tego rodzaju poza ramami wspólnotowymi.

75 — Zaznaczam, że temat związanych z trzecim filarem aspektów przekazywania danych osobowych przez przedsiębiorstwa lotnicze do Stanów Zjednoczonych bywa czasem podnoszony. Na przykład grupa robocza ds. ochrony danych (tzw. grupa artykułu 29) w opinii z dnia 24 października 2002 r. (opinia 6/2002 w sprawie przekazywania przez przedsiębiorstwa lotnicze informacji dotyczących pasażerów i członków załogi oraz innych danych do Stanów Zjednoczonych) wyraziła pogląd, że „[z]asadniczo przekazywanie danych z przeznaczeniem dla władz publicznych państwa trzeciego z powodów związanych z porządkiem publicznym tego państwa powinno być rozpatrywane w kontekście mechanizmów współpracy ustanowionych w ramach trzeciego filaru (współpraca sądowa i policyjna) [...]. Ważne jest, by unikać obchodzenia, via pierwszy filar, normalnych mechanizmów współpracy ustanowionych w trzecim filarze". Zobacz strona internetowa: http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2002_fr.htm.

władzami publicznymi [76]. To właśnie obowiązkowe ujawnianie danych do celów związanych z bezpieczeństwem i ściganiem przestępstw odgrywa ważniejszą rolę, nie zaś warunki, na jakich się odbywa w takiej czy innej sytuacji. Nasza sprawa w rzeczywistości dotyczy nowej problematyki, która wiąże się z wykorzystaniem danych handlowych do celów walki z przestępczością [77].

161. Na koniec należy podkreślić, że Trybunał orzekł, iż „walka z międzynarodowym terroryzmem [...] nie może być powiązana z żadnym z zadań wyraźnie wyznaczonych Wspólnocie w art. 2 WE oraz art. 3 WE" [78].

162. Zważywszy, że moja analiza zarzutu pierwszego doprowadziła do wniosku, by zaproponować Trybunałowi stwierdzenie nieważności decyzji Rady ze względu na błędny wybór podstawy prawnej decyzji, pozostałe zarzuty przedstawione przez Parlament na poparcie niniejszej skargi zbadam jedynie tytułem ewentualnym.

76 — Jeśli mowa o bezpośredniej wymianie informacji między władzami publicznymi, należy wymienić decyzję Rady z dnia 27 marca 2000 r. upoważniającą dyrektora Europolu do rozpoczęcia rokowań w sprawie umów z państwami trzecimi oraz instytucjami niepowiązanymi z UE (Dz.U. C 106, str. 1). Na tej podstawie została podpisana w dniu 20 grudnia 2002 r. umowa pomiędzy Europolem a Stanami Zjednoczonymi Ameryki w sprawie wymiany danych osobowych.

77 — Ta problematyka jest obecnie głównym przedmiotem dyskusji międzyinstytucjonalnej związanej z zatrzymywaniem danych przez dostawców usług telefonicznych i łączności elektronicznej. Rozbieżność stanowisk uczestników tej debaty, w której jedna ze stron wypowiada się za ujęciem tego zagadnienia w ramach pierwszego filaru, druga dla odmiany uważa, że wchodzi ono w zakres trzeciego filaru, świadczy o tym, że problematyka związana z wykorzystaniem danych z działalności gospodarczej do zwalczania przestępczości jest zagadnieniem nowym i równocześnie bardzo złożonym. Zobacz na ten temat projekt decyzji ramowej w sprawie zatrzymywania danych przetwarzanych i przechowywanych w związku ze świadczeniem publicznych usług łączności elektronicznej lub danych przekazywanych przez publiczne sieci łączności do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw, w tym także działalności terrorystycznej (projekt przedstawiony w dniu 28 kwietnia 2004 r. z inicjatywy Republiki Francuskiej, Irlandii, Królestwa Szwecji oraz Zjednoczonego Królestwa) oraz konkurencyjny projekt, autorstwa Komisji, dyrektywy Parlamentu Europejskiego i Rady w sprawie zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznych usług łączności elektronicznej, zmieniającej dyrektywę 2002/58, przedstawiony w dniu 21 września 2005 r. [COM(2005) 438 wersja ostateczna].

78 — Zobacz na temat nakładania sankcji gospodarczych i finansowych w postaci zamrożenia funduszy na osoby fizyczne i podmioty podejrzewane o udział w finansowaniu terroryzmu: wyroki Sądu z dnia 21 września 2005 r. w sprawie T-306/01 Yusuf i Al Barakaat International Foundation przeciwko Radzie i Komisji, Zb.Orz. str. II-3533, pkt 152, a także w sprawie T-315/01 Kadi przeciwko Radzie i Komisji, Zb.Orz. str. II-3649, pkt 116. W szczególnych okolicznościach tych spraw Sąd uwzględnił jednak „specjalnie ustanowiony w traktacie z Maastricht pomost między działaniami Wspólnoty nakładającymi sankcje gospodarcze na podstawie art. 60 WE i art. 301 WE oraz celami traktatu UE w zakresie stosunków zewnętrznych", pkt 159 wyroku w sprawie T-306/01 oraz pkt 123 wyroku w sprawie T-315/01). Bardziej ogólnie rzecz ujmując, stwierdził również, że „walka z międzynarodowym terroryzmem i jego finansowaniem bezspornie należy do celów Unii objętych WPZiB, zdefiniowanych w art. 11 UE [...]"., pkt 167 wyroku w sprawie T-306/01 oraz pkt 131 wyroku w sprawie T-315/01). Dodajmy, że zgodnie z art. 2 UE „Unia stawia sobie następujące cele: [...] utrzymanie i rozwijanie Unii jako przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której zagwarantowana jest swoboda przepływu osób, w powiązaniu z *właściwymi środkami w odniesieniu do* kontroli granic zewnętrznych, azylu, imigracji oraz *zapobieganie i zwalczanie przestępczości* [...]" (podkreślenie moje). Ponadto zgodnie z art. 29 akapit drugi UE cel Unii związany z zapewnieniem obywatelom wysokiego poziomu ochrony w przestrzeni wolności, bezpieczeństwa i sprawiedliwości „jest osiągany poprzez *zapobieganie i zwalczanie przestępczości zorganizowanej lub innej, zwłaszcza terroryzmu* [...]". (podkreślenie moje). Na temat zewnętrznego wymiaru europejskiej przestrzeni w dziedzinie prawa karnego, zob. G. Kerchove, A. Weyembergh, „Sécurité et justice: enjeu de la politique extérieure de l'Union européenne", éditions de l'Université de Bruxelles, 2003.

B — *W przedmiocie zarzutu opartego na naruszeniu art. 300 ust. 3 drugi akapit WE przez zmianę dyrektywy 95/46*

1. Argumenty stron

163. W zarzucie drugim Parlament podnosi, że porozumienie pomiędzy Wspólnotą a Stanami Zjednoczonymi mogło zostać zatwierdzone w imieniu Wspólnoty tylko według procedury określonej w art. 300 ust. 3 drugi akapit WE. Artykuł ten przewiduje, że „umowy powodujące zmianę aktu przyjętego według procedury określonej w artykule 251 są zawierane po uzyskaniu zgody Parlamentu Europejskiego". Tymczasem według tej instytucji przedmiotowe porozumienie pociąga za sobą konieczność zmiany dyrektywy 95/46, która została przyjęta z zastosowaniem procedury określonej w art. 251 WE.

164. Zdaniem Parlamentu zobowiązania, które władze amerykańskie według porozumienia zgodziły się wprowadzić w życie, nie spełniają wymogów w zakresie przetwarzania danych ustalonych w dyrektywie 95/46. W związku z tym porozumienie skutkuje wprowadzeniem odstępstw od niektórych podstawowych zasad wyżej wymienionej dyrektywy i zalegalizowaniem sposobów przetwarzania danych, które nie są przez nią dozwolone. W tym sensie porozumienie ma zmieniać dyrektywę 95/46. Parlament wskazuje w szczególności następujące zmiany.

165. Po pierwsze, celem porozumienia jest zapobieganie i zwalczanie terroryzmu oraz innych poważnych przestępstw, natomiast art. 3 ust. 2 tiret pierwsze dyrektywy 95/46 wyłącza z zakresu jej stosowania transfer danych z przeznaczeniem dla władz publicznych państwa trzeciego ze względów związanych z bezpieczeństwem publicznym tego państwa. Parlament podkreśla, że państwa członkowskie przewidziały do tego celu odpowiednie postanowienia w konwencji o Europolu i że można w związku z tym uznać, iż istnieje w tej dziedzinie komplementarność tych dwu instrumentów, które opierają się na różnych podstawach prawnych.

166. Po drugie, przyznana właściwym organom amerykańskim możliwość bezpośredniego dostępu do danych osobowych znajdujących się na obszarze Wspólnoty (system „pull") stanowi również zmianę dyrektywy 95/46, jako że art. 25 i 26 wyżej wymienionej dyrektywy nie zawierają żadnego przepisu zezwalającego, by państwo trzecie miało prawo bezpośredniego dostępu do tych danych.

167. Po trzecie, porozumienie przez odwołanie się do Zobowiązań ma zezwalać, aby CBP według własnego uznania w jednostkowych przypadkach mogło przekazywać dane

PNR rządowym organom ścigania lub powołanym do walki z terroryzmem spoza Stanów Zjednoczonych. Ta swoboda uznania pozostawiona władzom amerykańskim ma naruszać dyrektywę 95/46, a w szczególności art. 25 ust. 1, zgodnie z którym „przekazywanie do państwa trzeciego danych osobowych [...] mogło nastąpić tylko wówczas, gdy [...] dane państwo trzecie zapewni odpowiedni stopień ochrony". Parlament reprezentuje pogląd, iż faktycznie system ochrony wprowadzony przez omawianą dyrektywę zostałby zniweczony, gdyby państwo trzecie, w sprawie którego wydano pozytywną decyzję o odpowiedniej ochronie, miało później pełną swobodę w przekazywaniu danych osobowych innym państwom, które z kolei nie zostały poddane żadnej ocenie ze strony Komisji.

168. Po czwarte, porozumienie ma wprowadzać zmianę dyrektywy 95/46, ponieważ CBP, nawet jeżeli postanowi nie wykorzystywać tzw. wrażliwych danych osobowych, będzie prawnie upoważnione do ich zbierania, co stanowi już przetwarzanie w rozumieniu art. 2 lit. b) dyrektywy.

169. Po piąte, Parlament uważa, że porozumienie zmienia wyżej wymienioną dyrektywę, w zakresie w jakim prawo do korzystania ze środków prawnych w związku z naruszeniem praw zagwarantowanych każdej osobie przez przepisy krajowe dotyczące przetwarzania danych — prawo, o którym mowa w art. 22 dyrektywy 95/46 — nie jest dostatecznie zapewnione. W szczególności osoba, której dane PNR są przekazywane, nie posiada żadnej możliwości skorzystania ze środków prawnych na przykład w przypadku, gdyby dotyczące jej dane były niezgodne z prawdą, w razie wykorzystania danych wrażliwych lub przekazania danych innemu organowi.

170. Po szóste i ostatnie, Parlament podkreśla nadmiernie długi okres przechowywania danych PNR przekazanych CBP, co ma stanowić zmianę dyrektywy 95/46, a dokładniej jej art. 6 ust. 1 lit. e), który przewiduje okres przechowywania danych „nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane".

171. EIOD podziela opinię Parlamentu o tyle, że według niego porozumienie ma wpływ na dyrektywę 95/46. Jest on zdania, że porozumienie powinno być zawarte wyłącznie pod demokratyczną kontrolą Parlamentu, ponieważ dotyka kwestii harmonizacji ustawodawstw krajowych, o której mowa w tej dyrektywie, a nawet poszanowania praw podstawowych. Jego zdaniem obniżenie stopnia ochrony danych osobowych przewidzianego w dyrektywie wynika w szczególności z faktu, iż zarówno przy zastosowaniu systemu „pull", jak i systemu „push" przewoźnicy lotniczy są zmuszeni do działania z naruszeniem dyrektywy, w szczególności jej art. 6 ust. 1 lit. b) i c). Ponieważ takie naruszenie poziomu ochrony danych impli-

kuje zmianę dyrektywy 95/46, EIOD uważa, że gwarancje proceduralne, o których mowa w art. 300 ust. 3 drugi akapit WE, nie zostały dotrzymane. Ponadto stoi na stanowisku, że również gwarancje materialne nie zostały dotrzymane, przede wszystkim dlatego że zobowiązania CBP mają charakter niewiążący.

172. Natomiast Rada, popierana przez Komisję, reprezentuje podgląd, iż porozumienie nie implikuje zmiany dyrektywy 95/46. Na jego poparcie przywołuje pkt 8 porozumienia, w myśl którego „[c]elem tego porozumienia nie jest ani uchylenie, ani zmiana ustawodawstwa stron". Utrzymuje także, że dyrektywa ta daje Komisji szeroki zakres uznania przy ocenie odpowiedniego charakteru ochrony zapewnionego przez państwo trzecie. W tym względzie — zdaniem Rady — odpowiedź na pytanie, czy Komisja przekroczyła granice przysługującego jej swobodnego uznania stanowi raczej przedmiot skargi o stwierdzenie nieważności decyzji o odpowiedniej ochronie w sprawie C-318/04.

173. Rada przypomina również, że — według niej — motywy, jakimi kierowało się CBP (bezpieczeństwo, zwalczanie terroryzmu lub inne) wymagając przekazywania danych PNR, nie stanowią z punktu widzenia Wspólnoty ani celu, ani treści porozumienia. Ponadto dyrektywa 95/46 zezwala, by w zakresie stosowania w ramach rynku wewnętrznego dane osobowe mogły być wykorzystywane do uprawnionych celów, takich jak ochrona bezpieczeństwa państwa.

174. W każdym stanie rzeczy — według Rady — nawet przy założeniu, że Wspólnota nie miała kompetencji do zawarcia porozumienia, nie oznaczałoby to wcale, iż wymagana była zgoda Parlamentu z tego powodu, iż porozumienie zmienia dyrektywę 95/46. Jak bowiem zauważa Rada, zgoda Parlamentu w żadnym razie nie mogłaby skutkować rozszerzeniem zakresu kompetencji Wspólnoty.

175. Co do umożliwienia CBP bezpośredniego dostępu do danych PNR (system „pull", stosowany aktualnie w oczekiwaniu na wdrożenie systemu „push"), Rada wprawdzie przyznaje, że dyrektywa 95/46 nie wspomina wyraźnie takiej możliwości, ale też i nie zakazuje jej. Z punktu widzenia Wspólnoty ważniejsze są warunki dostępu do danych.

176. Komisja dodaje do tej argumentacji, że bez względu na cel, do jakiego dane osobowe są wykorzystywane przez CBP, nie zmienia to faktu, iż są one i pozostaną dla przewoźników lotniczych ze Wspólnoty danymi handlowymi podpadającymi pod dyrektywę 95/46 i w związku z tym powinny być chronione i przetwarzane zgodnie z dyrektywą.

2. Ocena

177. Przy zawieraniu umów międzynarodowych przez Wspólnotę konsultacje z Parlamentem należą niejako do procedury powszechnie stosowanej poza obszarem wspólnej polityki handlowej. Konsultacje z Parlamentem odbywają się na mocy art. 300 ust. 3 akapit pierwszy WE, włącznie z przypadkami gdy umowa dotyczy dziedziny, w której do przyjęcia wewnętrznych przepisów wymagana jest procedura współdecydowania określona w art. 251 WE.

178. Na zasadzie odstępstwa od tej reguły ogólnej art. 300 ust. 3 akapit drugi WE w czterech wypadkach wprowadza wymóg uzyskania zgody Parlamentu. Tym, który nas interesuje w niniejszej sprawie, jest przypadek umowy powodującej „zmianę aktu przyjętego według procedury określonej w artykule 251". Celem tego postanowienia jest zagwarantowanie, by Parlament jako współustawodawca miał kontrolę nad wprowadzeniem ewentualnych zmian do przyjętego przez niego aktu w drodze umowy międzynarodowej.

179. Dyrektywa 95/46 została przyjęta przy zastosowaniu procedury współdecydowania. Parlament twierdzi więc, że ponieważ porozumienie powodowało zmianę tejże dyrektywy, decyzja Rady zatwierdzająca to porozumienie w imieniu Wspólnoty wymagała jego zgody, aby została przyjęta zgodnie z zasadami przewidzianymi przez traktat.

180. Dla potrzeb oceny zasadności tego zarzutu przede wszystkim uściślę, że moim zdaniem nie ma wielkiego znaczenia postanowienie zawarte w pkt 8 porozumienia, stwierdzające, że „[c]elem tego porozumienia nie jest ani uchylenie, ani zmiana ustawodawstwa stron". W rzeczywistości tym, co jest ważne dla możliwości zastosowania art. 300 ust. 3 akapit drugi WE, jest ustalenie, czy umowa międzynarodowa *powoduje* zmianę wewnętrznego aktu wspólnotowego, tzn. czy *skutkuje* zmianą takiego aktu, bez względu na fakt, iż nie było to jej celem.

181. Co do powyższych stwierdzeń wydaje się, że do tej pory Trybunał nie wypowiadał się na temat sposobu rozumienia wyrażenia stosunkowo niedookreślonego „zmian[y] aktu przyjętego według procedury określonej w artykule 251" [79]. Niektórzy autorzy zastanawiali się nad kwestią, czy termin „zmiana" oznacza „zmianę niezgodną z brzmieniem" aktu wewnętrznego, czy też „każda zmiana, nawet w duchu dotychczasowego brzmienia" aktu wewnętrznego wystarczy, aby wymagać zastosowania procedury zgody Parlamentu [80].

79 — Natomiast Trybunał zajął już stanowisko w kwestii innego przypadku, gdzie wymagana jest zgoda Parlamentu, tj. „um[ów] mając[ych] istotne implikacje budżetowe dla Wspólnoty": wyrok z dnia 8 lipca 1999 r. w sprawie C-189/97 Parlament przeciwko Radzie, Rec. str. I-4741.

80 — Zobacz C. Schmitter, „Article 228", w: V. Constantinesco, R. Kovar, D. Simon, „Traité sur l'Union européenne, commentaire article par article", Economica, 1995, str. 725, zwłaszcza pkt 43.

182. Wyrażenie użyte w art. 300 ust. 3 akapit drugi WE nasuwa również pytanie, czy do tego, by wymagana była zgoda Parlamentu, zakres stosowania planowanej umowy powinien obejmować, przynajmniej częściowo, zakres przyjętego aktu wewnętrznego, czy też wystarczy sam fakt, iż akt wewnętrzny miał taką samą podstawę prawną, jaką zastosowano do zawarcia rzeczonej umowy [81].

183. Generalnie jestem zdania, że aby można było mówić o „zmianie" wewnętrznego aktu wspólnotowego przyjętego według procedury współdecydowania przez umowę międzynarodową, jednym z warunków jest, by zakres stosowania umowy pokrywał się z zakresem aktu wewnętrznego. W takim razie rzeczywiście zmiana aktu wewnętrznego umową międzynarodową może mieć miejsce albo dlatego że umowa zawiera postanowienie, które jest sprzeczne z przepisem aktu wewnętrznego, albo dlatego że umowa dodaje nową treść do aktu wewnętrznego, również wtedy gdy nie ma bezpośredniej sprzeczności.

184. W przypadku niniejszej sprawy uważam, że porozumienie nie mogło zmienić treści dyrektywy 95/46.

185. Swój pogląd opieram w pierwszej kolejności na fakcie, iż — jak wynika z mojej analizy zarzutu pierwszego — głównym celem porozumienia jest zwalczanie terroryzmu i innych poważnych przestępstw przy równoczesnym zapewnieniu ochrony danych osobowych pasażerów lotniczych. Natomiast dyrektywa 95/46 służy zapewnieniu swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi poprzez harmonizację przepisów krajowych służących ochronie osób fizycznych w odniesieniu do przetwarzania tego rodzaju danych. Obydwa akty mają zatem cele całkowicie różne, aczkolwiek obydwa dotyczą dziedziny ochrony danych osobowych [82].

186. Po drugie — co jest w pełni spójne z ustaleniem dotyczącym odrębności celów — okazuje się, że porozumienie i dyrektywa 95/46 mają różne zakresy stosowania. Otóż porozumienie stosuje się do przetwarzania danych osobowych do celów działalności na rzecz bezpieczeństwa wewnętrznego Stanów Zjednoczonych oraz, równocześnie i dokładniej rzecz ujmując, do działalności związanej ze zwalczaniem terroryzmu i innych poważnych przestępstw, natomiast przypominam, że art. 3 ust. 2 tiret pierwsze omawianej dyrektywy wyraźnie wyłącza ze swojego zakresu stosowania przetwarzanie 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*

81 — Zobacz podobnie C. Schmitter, op. cit.

82 — Zaznaczam, że rozwiązanie przyjęte w tym względzie przez Traktat ustanawiający konstytucję dla Europy jest rozszerzone i bardziej wzmacnia rolę zgody Parlamentu: art. III-325 traktatu, który dotyczy procedury zawierania umów międzynarodowych, w ust. 6 lit. a) ppkt v) przewiduje, że Rada przyjmuje decyzję w sprawie zawarcia umowy po uzyskaniu zgody Parlamentu w szczególności w przypadku „umów dotyczących *dziedzin*, do których stosuje się zwykłą procedurę ustawodawczą albo szczególną procedurę ustawodawczą, w przypadku której potrzebna jest zgoda Parlamentu Europejskiego" (podkreślenie moje).

razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarcza państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz *działalności państwa w obszarach prawa karnego*" [83].

187. Zważywszy na fakt, iż w rozpoznawanej sprawie obydwa akty mają różne cele i zakresy stosowania, nie widzę możliwości, by treść jednego z nich była w stanie zmienić drugi. Prawdę powiedziawszy porozumienie dotyczy przetwarzania danych osobowych, co do którego ustawodawca wspólnotowy wyraźnie wykluczył możliwość objęcia go systemem ochrony utworzonym przez dyrektywę 95/46. Takie rozwiązanie przyjęte przez ustawodawcę wspólnotowego jest zresztą spójne z wyborem podstawy prawnej dyrektywy, tj. art. 95 WE.

188. Sądzę, że tej analizy nie jest w stanie podważyć argument Komisji, która utrzymuje, iż bez względu na cel, do jakiego dane osobowe są wykorzystywane przez CBP, pozostaje faktem, iż są one i pozostaną dla przewoźników lotniczych ze Wspólnoty danymi handlowymi podpadającymi pod dyrektywę 95/46 i w związku z tym powinny być chronione i przetwarzane zgodnie z dyrektywą.

189. Przypominam w tym względzie, że o ile prawdą jest, iż operacja przetwarzania, jaką stanowi gromadzenie i rejestrowanie danych pasażerów lotniczych przez przedsiębiorstwa lotnicze, ma generalnie cel gospodarczy, w zakresie w jakim jest bezpośrednio związana z przebiegiem lotu obsługiwanego przez przewoźnika lotniczego, o tyle jednak przetwarzanie danych regulowane przez porozumienie ma całkowicie odmienny charakter, gdyż z jednej strony obejmuje etap późniejszy od gromadzenia danych, z drugiej zaś służy celom związanym z bezpieczeństwem.

190. W świetle całości powyższych stwierdzeń wyrażam pogląd, iż zarzut drugi podniesiony przez Parlament jest bezzasadny, a zatem należy go oddalić.

191. Z tych samych powodów, które zostały przedstawione powyżej przy badaniu sprawy C-318/04 [84], zajmę się teraz analizowaniem łącznie zarzutów trzeciego i czwartego Parlamentu, tj. naruszenia prawa do ochrony danych osobowych oraz naruszenia zasady proporcjonalności.

83 — Podkreślenie moje.

84 — Punkt 107 niniejszej opinii.

192. Przypominam również, że z uwagi na wzajemne zależności pomiędzy porozumieniem zatwierdzonym decyzją Rady, decyzją o odpowiedniej ochronie oraz Zobowiązaniami CBP stanowiącymi załącznik do wyżej wymienionej decyzji Komisji, uważam, że to cały system PNR powinien być poddany analizie pod kątem tych zarzutów [85].

C — *W przedmiocie zarzutów opartych na naruszeniu prawa do ochrony danych osobowych oraz naruszeniu zasady proporcjonalności*

1. Argumenty stron

193. Parlament utrzymuje, że system PNR narusza prawo do ochrony danych osobowych, które zostało uznane w szczególności przez art. 8 EKPC.

194. Według Parlamentu fakt, iż porozumienie przewiduje, że CBP może mieć dostęp drogą elektroniczną do danych PNR pochodzących z systemów rezerwacji przewoźników lotniczych znajdujących się na terytorium państw członkowskich, a także iż zawiera postanowienia, że wyżej wymienieni przewoźnicy, kiedy świadczą usługi międzynarodowego przewozu pasażerów do i ze Stanów Zjednoczonych, muszą przetwarzać dane PNR zgodnie z wymaganiami CBP odpowiednio do prawa amerykańskiego, decyduje o tym, że przedmiotem porozumienia jest przetwarzanie danych osobowych, które stanowi ingerencję w życie prywatne w rozumieniu art. 8 EKPC. Także decyzja o odpowiedniej ochronie narusza ten artykuł.

195. Parlament uścisla, że aby nie stanowić naruszenia art. 8 EKPC, tego rodzaju ingerencja powinna być przewidziana przez ustawę, służyć celowi zgodnemu z prawem i być konieczna w demokratycznym społeczeństwie do osiągnięcia tego celu. Stoi on na stanowisku, że porozumienie i decyzja o odpowiedniej ochronie nie spełniają tych warunków.

196. Po pierwsze, co do warunku, zgodnie z którym ingerencja musi być przewidziana przez ustawę, Parlament zwraca uwagę, że zarówno porozumienie, jak i decyzja o odpowiedniej ochronie nie spełniają warunków dostępności i przewidywalności prawa, których wymaga orzecznictwo Europejskiego Trybunału Praw Człowieka. Z jednej strony, w kwestii warunku dostępności prawa, Parlament uważa, że przez ogólne i nieprecyzyjne odesłanie do obowiązującego amerykańskiego ustawodawstwa, porozumienie i decyzja o odpowiedniej ochronie same nie zawierają praw i obowiązków pasażerów i europejskich linii lotniczych. Tymczasem zasada pewności prawa wymaga, by akt wspólnotowy, który tworzy obowiązki prawne, umożliwiał zainteresowanym dokładne zapoznanie się

85 — Zobacz pkt 109 i nast. niniejszej opinii.

z zakresem obowiązków, które na nich nakłada [86]. Ponadto wbrew temu, czego wymaga warunek dostępności, obowiązujące ustawy amerykańskie nie są dostępne we wszystkich językach oficjalnych Wspólnoty. Parlament zauważył również błąd w preambule porozumienia dotyczący numeru oraz daty przyjęcia decyzji o odpowiedniej ochronie. Z drugiej strony, jeśli chodzi o warunek przewidywalności prawa, jest on niespełniony, gdyż decyzja o odpowiedniej ochronie nie zawiera z wystarczającą precyzją określonych praw i obowiązków przedsiębiorstw lotniczych oraz obywateli z krajów Wspólnoty. Ponadto pasażerowie otrzymują tylko informację ogólną, co jest sprzeczne z obowiązkiem informowania, o którym mowa w art. 10 i 11 dyrektywy 95/46 oraz w art. 8 lit. a) konwencji 108. Wreszcie porozumienie i Zobowiązania CBP zawierają szereg nieścisłości niezgodnych z wymogami art. 8 EKPC.

197. Po drugie, w kwestii warunku, według którego zgodnie z art. 8 ust. 2 EKPC ingerencja w prawo do poszanowania życia prywatnego musi służyć uprawnionemu celowi, Parlament przyznaje, że został on spełniony. Przypomina też, iż wielokrotnie wyrażał swoje poparcie dla Rady w walce z terroryzmem.

198. Po trzecie, co do warunku wymagającego, by ingerencja stanowiła środek, który w społeczeństwie demokratycznym jest konieczny z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia lub moralności lub ochronę praw i wolności innych osób, Parlament uważa, że nie został on spełniony z następujących przyczyn:

— z ust. 3 Zobowiązań CBP wynika, że przetwarzanie danych nie ogranicza się wyłącznie do celów zwalczania terroryzmu, ale służy również do zapobiegania i zwalczania innych poważnych przestępstw, włącznie z przestępczością zorganizowaną oraz ucieczką w przypadku nakazu aresztowania lub pozbawienia wolności za powyższe przestępstwa. W zakresie w jakim przetwarzanie danych wykracza poza samą walkę z terroryzmem, nie jest — zdaniem Parlamentu — konieczne do realizacji uprawnionego celu, któremu ma służyć;

— porozumienie przewiduje transfer zbyt dużej liczby elementów danych (34), a tym samym nie stosuje się do zasady proporcjonalności. Z punktu widzenia zapewniania odpowiedniego poziomu ochrony danych osobowych tylko 19 z tych 34 pozycji wydaje się do zaakceptowania. Parlament uważa, że istnieje „znaczna różnica" pomiędzy ilością danych przewidzianą w porównywalnych aktach prawnych obowiązujących

86 — Parlament powołuje się w tej kwestii na wyrok z dnia 20 maja 2003 r. w sprawie C-108/01 Consorzio del Prosciutto di Parma i Salumificio S.Rita, Rec. str. I-5121, pkt 89.

na szczeblu Unii Europejskiej a wymaganą na mocy porozumienia [87]. Ponadto niektóre żądane elementy danych PNR mogą zawierać tzw. dane wrażliwe;

— porozumienie nie przewiduje kontroli sądowej w związku z przetwarzaniem danych przez władze amerykańskie. Co więcej, ponieważ porozumienie i Zobowiązania nie tworzą praw na rzecz osób, których dane osobowe są przetwarzane, Parlament nie widzi, w jaki sposób te osoby mogłyby ich dochodzić przed sądami amerykańskimi;

— dane są przechowywane przez władze amerykańskie przez okres zbyt długi w stosunku do potrzeb realizowanego celu. Faktycznie ze Zobowiązań CBP wynika, że w związku tym że uprawnione osoby z CBP mają mieć dostęp on-line do danych zawartych w PNR przez okres 7 dni, wszystkie dane są przechowywane przez okres trzech lat i sześciu miesięcy. Następnie dane, do których uzyskano ręcznie dostęp w trakcie tego okresu, zostaną przekazane przez CBP do pliku skasowanych danych w postaci pierwotnej, gdzie pozostaną przez okres ośmiu lat przed ich całkowitym zniszczeniem. Porównanie z systemami informacyjnymi utworzonymi na przykład w ramach konwencji wykonawczej do układu z Schengen, konwencji o Europolu oraz decyzji o Eurojuście, gdzie okres przechowywania ustalono na rok do trzech lat, wykazuje, iż okres przyjęty w Zobowiązaniach jest nadmiernie długi;

— porozumienie umożliwia przekazywanie danych innym władzom publicznym; w ten sposób wykracza poza zakres tego, co konieczne do celów walki z terroryzmem.

199. Z kolei EIOD broni tezy, iż przetwarzanie 6 kategorii danych stanowi oczywiste naruszenie prawa do życia prywatnego [88]. Naruszenie wynika również jego zdaniem z możliwości tworzenia profili osobowych na podstawie tych danych. EIOD popiera argumenty Parlamentu wykazujące, że ingerencja jest nieuzasadniona w świetle art. 8 ust. 2 EKPC. Uważa również, że stopień ochrony oferowany przez CBP nie jest odpowiedni w rozumieniu art. 25 dyrektywy 95/46,

87 — Parlament wymienia tu w szczególności konwencję o Europolu, która w art. 8 ust. 2 przewiduje przetwarzanie pięć danych, a także dyrektywę 2004/82/WE Rady z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (Dz.U. L 261, str. 24). Dyrektywa ta, której podstawą prawną jest art. 62 ust. 2 lit. a) WE oraz art. 63 ust. 3 lit. b) WE, w art. 3 określa zobowiązanie dla przewoźników lotniczych do przesyłania na wniosek organów odpowiedzialnych za przeprowadzanie kontroli osób na granicach zewnętrznych, danych osobowych obejmujących w sumie dziewięć elementów.

88 — Dotyczy to zdaniem EIOD elementów o numerach: 11 — „Informacje dotyczące osoby często podróżującej (ograniczone do ilości przelecianych mil i adresu(-ów))"; 19 — „Uwagi ogólne"; 26 — „Informacja OSI (inn[e] usług[i])"; 27 — „Informacja SSI/SSR (specjalne usługi)"; 30 — „Liczba podróżujących w ramach danego PNR" oraz 33 — „Wszelkie zebrane informacje APIS (Advanced Passenger Information System)".

przede wszystkim dlatego że art. 8 EKPC nie jest przestrzegany.

200. Natomiast Rada i Komisja uważają, że system PNR spełnia warunki określone w art. 8 ust. 2 EKPC, zgodnie z wykładnią dokonaną przez Europejski Trybunał Praw Człowieka.

201. Po pierwsze, co do warunku, zgodnie z którym ingerencja musi być przewidziana przez ustawę, Rada stoi na stanowisku, że do spełnienia warunku dostępności prawa nie jest konieczne, by tekst porozumienia zawierał wszystkie przepisy, które mogłyby ewentualnie odnosić się do osób zainteresowanych. Nie jest sprzeczne z prawem, by porozumienie zawierało odesłanie do decyzji o odpowiedniej ochronie oraz do zobowiązań CBP ujętych w załączniku do decyzji, ponieważ wszystkie te akty zostały ogłoszone w *Dzienniku Urzędowym Unii Europejskiej*. Ponadto dziennik ten nie jest przeznaczony do publikowania przepisów prawa państw trzecich. W kwestii błędnego numeru decyzji o odpowiedniej ochronie zawartego w preambule porozumienia Rada poinformowała, że wyda odpowiednie polecenia, aby sprostowanie ukazało się w Dzienniku Urzędowym, uważa jednak, iż jest to błąd natury technicznej, niemający wpływu na dostępność rzeczonego aktu prawnego w rozumieniu orzecznictwa Europejskiego Trybunału Praw Człowieka. W odniesieniu do zasady przewidywalności prawa Rada reprezentuje pogląd, iż nie została ona naruszona przez fakt, że zobowiązania CBP ani amerykańskie ustawy i wymogi konstytucyjne nie były przytoczone in extenso w samym porozumieniu. Ponadto zobowiązania CBP są sformułowane wystarczająco precyzyjnie, by umożliwiać osobom, których dotyczą, odpowiednie regulowanie swoich zachowań.

202. Po drugie, w kwestii przesłanki, według której ingerencja musi służyć legalnemu celowi, Rada zaznacza, że zwalczanie poważnych przestępstw innych niż terroryzm wchodzi w zakres kilku kategorii uprawnionych interesów, o których mowa w art. 8 ust. 2 EKPC (w szczególności bezpieczeństwa publicznego, ochrony porządku i zapobiegania przestępstwom). W związku z tym porozumienie i Zobowiązania CBP służą uprawnionemu celowi również w zakresie dotyczącym innych poważnych przestępstw.

203. Po trzecie, Rada uważa, że ingerencja jest proporcjonalna w stosunku do zamierzonego celu. Dokładniej rzecz ujmując twierdzi, że dane PNR wymagane przez CBP są potrzebne do zapobiegania aktom terroryzmu lub przestępczości zorganizowanej, a także dostarczenia materiału dla śledztw wszczętych w związku z zamachami, przez ułatwienie identyfikacji osób powiązanych z grupami terrorystycznymi lub z przestępczością zorganizowaną. Co się tyczy ilości przekazywanych elementów danych PNR, porównanie z systemami informacyjnymi w Unii Europejskiej nie jest właściwe, ponieważ pomijając fakt, że systemy te mają inny cel oraz zawartość niż system PNR, konieczność sporządzenia profilu potencjalnego terrorysty wymaga dostępu do większej ilości danych. Jeśli chodzi o trzy elementy danych PNR, które zdaniem Parlamentu mogą zawierać tzw.

dane wrażliwe [89], Rada zwraca uwagę, że dostęp CBP do tych trzech pozycji został ściśle ograniczony na podstawie ust. 5 zobowiązań podjętych przez CBP [90]. Co więcej, zgodnie ze zobowiązaniami w zawartymi punktach 9, 10 i 11, w każdym wypadku jest wykluczone, by CBP mogło wykorzystywać dane wrażliwe [91]. W kwestii długości okresu przechowywania danych PNR Rada stoi na stanowisku, że wziąwszy pod uwagę fakt, iż śledztwa w sprawie zamachów trwają niekiedy wiele lat, normalny okres przechowywania ustalony na trzy i pół roku, z wyłączeniem szczególnych przypadków, kiedy ten okres może być dłuższy, stanowi wyważone rozwiązanie. Ponadto nie ma powodów, by sądzić, że brak jest niezależnego systemu kontroli. Na koniec transfer danych do innych organów publicznych jest objęty wystarczającymi gwarancjami; przede wszystkim CBP może przekazywać dane innym organom publicznym tylko w jednostkowych przypadkach i do celów zapobiegania lub zwalczania terroryzmu i innych poważnych przestępstw.

204. Zdaniem Komisji nie ma wątpliwości, że pakiet przepisów, jaki tworzą porozumienie, decyzja o odpowiedniej ochronie i Zobowiązania CBP, dopuszcza możliwość pewnej ingerencji w życie prywatne, różnego stopnia w zależności od przekazywanych danych. Tego rodzaju ingerencja, według Komisji, została przewidziana przez ustawę, tzn. wyżej wymieniony pakiet aktów; służy do uprawnionego celu, tj. do usunięcia kolizji norm powstałej pomiędzy amerykańskimi przepisami związanymi z ochroną bezpieczeństwa a przepisami wspólnotowymi dotyczącymi ochrony danych osobowych, a także jest konieczna w demokratycznym społeczeństwie do osiągnięcia tego celu.

205. Zjednoczone Królestwo reprezentuje pogląd, że dla potrzeb badania ewentualnego naruszenia prawa do ochrony danych osobowych decyzja Rady, porozumienie, decyzja o odpowiedniej ochronie oraz Zobowiązania CBP powinny być analizowane razem, ponieważ stanowią instrumenty prawne ściśle powiązane. Uważa również, że pod kątem dostępności i przewidywalności należy zbadać prawo wspólnotowe obowiązujące w tej dziedzinie, a nie ustawodawstwo obowiązujące na terytorium Stanów Zjednoczonych. Jeśli zestawić razem porozumienie, decyzję o odpowiedniej ochronie oraz Zobowiązania CBP, prawo wspólnotowe zawierać będzie zdaniem Zjednoczonego Królestwa jasny i pełny obraz sytuacji prawnej wszystkich

89 — Dotyczy pozycji nr 19, 26 i 27 (zobacz poprzedni przypis).

90 — Ustęp 5 Zobowiązań stanowi:
„W odniesieniu do danych określonych jako »OSI« i »SSI/SSR« (potocznie określane jako uwagi ogólne i pola otwarte) zautomatyzowany system CBP będzie przeszukiwał wymienione pola w poszukiwaniu innych danych określonych [na liście wymaganych elementów danych PNR]. Personel CBP nie będzie upoważniony do ręcznego przeglądania wszystkich informacji pól OSI i SSI/SSR, jeżeli osoba, której dotyczą dane zawarte w PNR, nie została określona przez CBP jako osoba o wysokim ryzyku w odniesieniu do jakiegokolwiek celu określonego w ust. 3 niniejszego dokumentu".

91 — Ustęp 9 Zobowiązań przewiduje:
„CBP nie będzie wykorzystywać »danych szczególnie chronionych [wrażliwych]« (tzn. danych osobowych wskazujących na pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne lub przynależność do związków zawodowych oraz danych dotyczących zdrowia i życia seksualnego) zawartych w PNR, jak opisano poniżej".
Ustęp 10 Zobowiązań stanowi:
„CBP wprowadzi w życie, możliwie najszybciej, zautomatyzowany system filtrujący i usuwający niektóre szczególnie chronione kody i określenia zawarte w PNR, określone przez CBP w porozumieniu z Komisją".
Ustęp 11 Zobowiązań ma następujące brzmienie:
„Do czasu wprowadzenia w życie takich filtrów CBP deklaruje, że nie wykorzystuje i nie będzie wykorzystywać szczególnie chronionych danych zawartych w PNR oraz zobowiązuje się do usunięcia takich danych z wszelkich przypadków uznaniowego ujawnienia PNR na mocy ust. 28–34".
Wskazane powyżej ustępy Zobowiązań dotyczą przekazywania danych PNR innym organom rządowym.

podmiotów, których dotyczy. Ponadto nie podziela ono opinii, że zobowiązania CBP mają charakter jednostronny i mogą zostać zmienione lub wypowiedziane przez władze amerykańskie bez żadnych konsekwencji.

206. W kwestii konieczności ingerencji Zjednoczone Królestwo podkreśla przede wszystkim, że zwalczanie innych poważnych przestępstw jest wyraźnie wskazane jako cel porozumienia i stanowi cel związany z porządkiem publicznym równie uprawniony jak walka z terroryzmem. Zjednoczone Królestwo uważa też, że zestaw danych, które mogą być przekazywane, okres ich przetrzymywania oraz możliwość dalszego przekazania innym organom odpowiadają tym celom i są do nich proporcjonalne, zwłaszcza wziąwszy pod uwagę liczne gwarancje, jakie zawarto w Zobowiązaniach i w decyzji o odpowiedniej ochronie w celu ograniczenia zagrożeń dla prawa do prywatności pasażerów. Na koniec dodaje, że jego zdaniem kryterium proporcjonalności powinno być stosowane w sposób zgodny równocześnie z orzecznictwem Trybunału Sprawiedliwości oraz Europejskiego Trybunału Praw Człowieka w świetle charakteru i wagi celów, o których mowa.

2. Ocena

207. W tych zarzutach Parlament utrzymuje, że decyzja Rady oraz decyzja o odpowiedniej ochronie naruszają prawo do ochrony danych osobowych zagwarantowane w szczególności w art. 8 EKPC.

208. Zgodnie z utrwalonym orzecznictwem prawa podstawowe stanowią integralną część ogólnych zasad prawa, których poszanowanie zapewnia Trybunał [92]. W tym celu Trybunał kieruje się tradycjami konstytucyjnymi wspólnymi dla państw członkowskich, a także wskazówkami, jakich dostarczają międzynarodowe akty prawne dotyczące ochrony praw człowieka, które państwa członkowskie współtworzyły lub do nich przystąpiły. Uważa też, że EKPC ma w tym względzie „szczególne znaczenie" [93]. Zatem nie mogą być przyjęte we Wspólnocie środki nie dające się pogodzić z poszanowaniem praw człowieka tą drogą uznanych i zagwarantowanych [94]. Zasady te zostały ujęte w art. 6 ust. 2 UE.

209. W miarę rozwoju tego kierunku orzecznictwa Trybunał włączył do kanonu

92 — Zobacz w szczególności wyroki: z dnia 12 listopada 1969 r. w sprawie 29/69 Stauder, Rec. str. 419, pkt 7; z dnia 17 grudnia 1970 r. w sprawie 11/70 Internationale Handelsgesellschaft, Rec. str. 1125, pkt 4, oraz z dnia 14 maja 1974 r. w sprawie 4/73 Nold przeciwko Komisji, Rec. str. 491, pkt 13.

93 — Zobacz w szczególności wyroki z dnia 18 czerwca 1991 r. w sprawie C-260/89 ERT, Rec. str. I-2925, pkt 41; z dnia 29 maja 1997 r. w sprawie C-299/95 Kremzow, Rec. str. I-2629, pkt 14, oraz z dnia 6 marca 2001 r. w sprawie C-274/99 P Connolly przeciwko Komisji, Rec. str. I-1611, pkt 37.

94 — Wyrok z dnia 13 lipca 1989 r. w sprawie 5/88 Wachauf, Rec. str. 2609, pkt 19.

wymogów praworządności wspólnotowej także prawo do poszanowania życia prywatnego [95]. Prawo do ochrony danych osobowych stanowi jeden z elementów prawa do poszanowania życia prywatnego, zatem podlega ochronie z art. 8 EKPC, również we wspólnotowym porządku prawnym, przez pryzmat ogólnych zasad prawa.

210. Zbadam teraz, czy system PNR stanowi naruszenie prawa do poszanowania życia prywatnego, postępując według schematu analizy wynikającego z brzmienia art. 8 EKPC. Zatem po ustaleniu, czy ten system stanowi ingerencję w życie prywatne pasażerów lotniczych, zajmę się ustaleniem, czy ingerencja ta była należycie usprawiedliwiona.

a) W przedmiocie istnienia ingerencji w życie prywatne

211. Fakt, iż doszło do ingerencji w życie prywatne przez pakiet aktów, który tworzą decyzja Rady zatwierdzająca porozumienie, decyzja o odpowiedniej ochronie oraz Zobowiązania CBP, moim zdaniem nie budzi żadnych wątpliwości. Wydaje mi się bowiem oczywiste, że wgląd do danych, wykorzystywanie przez CBP oraz udostępnianie mu danych pasażerów lotniczych pochodzących z systemów rezerwacji przewoźników lotniczych znajdujących się na obszarze państw członkowskich jest ze strony władz publicznych wtargnięciem w życie prywatne pasażerów.

212. Dodam też, że fakt, iż ingerencja w życie prywatne pasażerów lotniczych miała miejsce, wydaje się wykazany, chociaż niektóre elementy danych PNR, potraktowane oddzielnie, mogłyby zostać uznane za samodzielnie nienaruszające prywatności pasażerów, których dotyczą. Dlatego sądzę, iż należy koniecznie całościowo rozpatrywać listę danych PNR wymaganych przez CBP, jako że zestawienie tych danych jest w stanie umożliwić tworzenie profili osobowych.

213. Ingerencja w życie prywatne narusza prawo do prywatności, chyba że jest należycie usprawiedliwiona.

b) W przedmiocie uzasadnienia ingerencji w życie prywatne

214. Dopuszczalność ingerencji w życie prywatne jest uzależniona od spełnienia trzech

95 — Wyrok z dnia 26 czerwca 1980 r. w sprawie 136/79 National Panasonic przeciwko Komisji, Rec. str. 2033, pkt 18 i 19. Prawo to obejmuje także prawo do ochrony tajemnicy lekarskiej [zobacz wyroki z dnia 8 kwietnia 1992 r. w sprawie C-62/90 Komisja przeciwko Niemcom, Rec. str. I-2575, oraz z dnia 5 października 1994 r. w sprawie C-404/92 P X przeciwko Komisji, Rec. str. I-4737)]. Jeśli chodzi o prawo do ochrony danych osobowych, ponownie zwracam uwagę na ww. wyroki w sprawach Österreichischer Rundfunk i in. oraz Lindqvist.

przesłanek: ingerencja musi być przewidziana przez ustawę, musi służyć uprawnionemu celowi i stanowić konieczność w demokratycznym społeczeństwie.

i) Czy ingerencja była przewidziana przez ustawę?

215. Według utrwalonego orzecznictwa Europejskiego Trybunału Praw Człowieka przesłanka ta wymaga, by dany środek miał podstawę prawną i dotyczy również przymiotów przedmiotowej ustawy [96]. Ocena przymiotów ustawy pociąga za sobą konieczność, by była ona dostępna dla obywateli, precyzyjna i przewidywalna co do konsekwencji. W związku z tym ustawa musi określać wystarczająco wyraźnie zakres i sposób ograniczenia zagwarantowanego obywatelowi prawa, aby umożliwić mu odpowiednie regulowanie swojego zachowania oraz korzystanie z należytej ochrony przed arbitralnością [97].

216. Parlament utrzymuje, że środek przewidujący ingerencję nie jest ani dostępny, ani przewidywalny pod względem jego konsekwencji. Nie podzielam tej opinii.

217. Wręcz przeciwnie, moim zdaniem lektura decyzji Rady i załączonego do niej porozumienia, a także decyzji o odpowiedniej ochronie, która zawiera w załączniku Zobowiązania CBP, pozwala podmiotom, których te akty dotyczą, tj. przedsiębiorstwom lotniczym oraz pasażerom lotniczym, być poinformowanym wystarczająco dokładnie, aby odpowiednio regulować swoje zachowania.

218. Pozwolę sobie zauważyć w tym miejscu, że Zobowiązania CBP obejmujące 48 ustępów, są stosunkowo szczegółowe i dostarczają dokładnych informacji na temat obowiązującego stanu prawnego. Co więcej, decyzja o odpowiedniej ochronie wymienia w preambule amerykańską ustawę obowiązującą w tym zakresie oraz przepisy wykonawcze przyjęte przez CBP na mocy tej ustawy [98]. W związku z tym uważam za przesadne wymaganie, by obowiązujące amerykańskie przepisy ustawowe i wykonawcze były jeszcze publikowane w całości w *Dzienniku Urzędowym Unii Europejskiej*. Poza tym, że — jak nadmieniła Rada — nie jest on przeznaczony do publikowania przepisów prawa państw trzecich, jestem zdania, że Zobowiązania CBP, które zostały ogłoszone w Dzienniku Urzędowym, zawierają istotne informacje na temat procedury wykorzystywania danych przez CBP oraz towarzyszących jej gwarancji.

96 — Wyrok ETPC z dnia 24 kwietnia 1990 r. w sprawie Kruslin przeciwko Francji (seria A, nr 176-A, § 27).

97 — Wyrok ETPC z dnia 24 marca 1988 r. w sprawie Olsson przeciwko Szwecji (seria A, nr 130, § 61 i 62). Ograniczenia muszą być przewidziane przez przepisy prawa sformułowane w sposób wystarczająco precyzyjny, by umożliwić zainteresowanym odpowiednie regulowanie zachowania przez zasięgnięcie w razie potrzeby fachowej porady [wyrok ETPCz z dnia 26 kwietnia 1979 r. w sprawie Sunday Times przeciwko Wielkiej Brytanii (seria A, nr 30, § 49)].

98 — Zobacz motyw szósty decyzji o odpowiedniej ochronie oraz przypisy 2 i 3.

219. Zgodnie z zasadą pewności prawa przedsiębiorstwa lotnicze, które obejmuje system PNR, są informowane o obowiązkach nałożonych na nie na mocy porozumienia, a pasażerowie lotniczy są informowani o swoich prawach, w szczególności w kwestii dostępu do danych i ich sprostowania [99].

220. Z pewnością biorąc pod uwagę wzajemne zależności między elementami składającymi się na system PNR, należy ubolewać nad błędami w preambule porozumienia dotyczącymi numeru i daty wydania decyzji o odpowiedniej ochronie. Faktycznie pomyłki te komplikują sytuację obywatela europejskiego, który chciałby uzyskać informacje o zasadach systemu uzgodnionego ze Stanami Zjednoczonymi. Jednakże według mnie nie utrudniają one nadmiernie poszukiwania informacji, gdyż decyzja o odpowiedniej ochronie została ogłoszona w Dzienniku Urzędowym, a narzędzia do wyszukiwania, zwłaszcza informatyczne, pozwalają łatwo ją znaleźć. Ponadto Rada zobowiązała się do opublikowania w Dzienniku Urzędowym sprostowania, co zostało faktycznie zrobione [100].

221. W świetle powyższych stwierdzeń uważam, że ingerencja w życie prywatne pasażerów lotniczych, których dotyczy, powinna być uznana za „przewidzianą przez ustawę" w rozumieniu art. 8 ust. 2 EKPC.

99 — Zobacz ust. 36–42 Zobowiązań.

100 — Zobacz Protokół ze sprostowania do Porozumienia, który — przypominam — ukazał się w Dz.U. L 255 z dnia 30 września 2005 r.

ii) Czy ingerencja służy uprawnionemu celowi?

222. Wziąwszy pod uwagę różne cele wymienione w art. 8 ust. 2 EKPC, uważam, że ingerencja w życie prywatne, będąca przedmiotem niniejszej sprawy, miała uprawniony cel. W szczególności odnosi się to do zwalczania terroryzmu.

223. Podobnie jak Rada sądzę, że zwalczanie poważnych przestępstw innych niż terroryzm [101] również wchodzi w zakres kilku kategorii uprawnionych interesów, o których mowa w art. 8 ust. 2 EKPC, jak np. bezpieczeństwo publiczne, ochrona porządku czy zapobieganie przestępstwom. W związku z tym uważam, że system PNR służy uprawnionemu celowi również wtedy, kiedy odnosi się do innych poważnych przestępstw.

224. Obecnie należy zbadać kwestię proporcjonalności ingerencji przez ustalenie odpowiedzi na pytanie, czy jest ona konieczna w demokratycznym społeczeństwie w celu zapobiegania terroryzmowi i innym poważnym przestępstwom i zwalczania ich.

101 — Przypominam, że w preambule porozumienia wymieniono zapobieganie terroryzmowi „i związany[m] z nim przestępstw[om] oraz inny[m] poważny[m] przestępstw[om], o ponadnarodowym charakterze, włącznie z przestępczością zorganizowaną [i zwalczanie ich]". Ponadto ust. 3 Zobowiązań stanowi, że „[d]ane zawarte w PNR są wykorzystywane przez CBP wyłącznie do celów zapobiegania [...] 1) terroryzm[owi] i związany[m] z nim przestępstw[om]; 2) inny[m] poważny[m] przestępstw[om], włącznie z przestępczością zorganizowaną, która z zasady ma charakter transnarodowy [i zwalczania ich]; oraz 3) unikani[u] kary aresztu lub więzienia za powyższe przestępstwa". Podobnie zobacz także motyw piętnasty decyzji o odpowiedniej ochronie.

iii) Czy ingerencja jest konieczna w demokratycznym społeczeństwie do osiągnięcia takiego celu?

225. Przed przystąpieniem do dokładnego badania pod kątem przestrzegania zasady proporcjonalności przedstawię kilka uwag wstępnych na temat zakresu kontroli wykonywanej przez Trybunał.

226. Według Europejskiego Trybunału Praw Człowieka przymiotnik „konieczny", w rozumieniu art. 8 ust. 2 EKPC, zakłada istnienie „naglącej potrzeby społecznej" oraz że podjęty środek jest „proporcjonalny do zamierzonego uprawnionego celu" [102]. Ponadto „władzom krajowym przyznano pewien margines swobody, którego zakres zależy nie tylko od celu, ale również od stopnia ingerencji" [103].

227. W ramach kontroli marginesu swobody uznania pozostawionego państwom Europejski Trybunał Praw Człowieka tradycyjnie bada, czy powody, na które powołano się dla usprawiedliwienia ingerencji są adekwatne i wystarczające, następnie czy ingerencja jest proporcjonalna do realizowanego uprawnionego celu i ocenia, czy została zachowana równowaga pomiędzy interesem powszechnym a interesami jednostki [104]. Na podstawie tego orzecznictwa można dojść do wniosku, że „[z]asada proporcjonalności, która wyraża wymóg adekwatności uprawnionego celu oraz środków użytych do jego osiągnięcia, zajmuje centralne miejsce w kontroli marginesu uznania pozostawionego władzom krajowym" [105].

228. Kontrola proporcjonalności dokonywana przez Europejski Trybunał Praw Człowieka jest różna w zależności od parametrów takich jak istota prawa i rodzaj działalności w rozpoznawanej sprawie, cel ingerencji oraz ewentualna obecność wspólnego mianownika systemów prawnych państw.

229. Co do istoty prawa i rodzaju działalności w rozpoznawanej sprawie, kiedy chodzi o prawo, które blisko dotyka sfery intymności jednostki, takie jak prawo do poufności danych osobowych związanych ze zdrowiem [106], Europejski Trybunał Praw Czło-

102 — Zobacz w szczególności wyrok ETPC z dnia 24 listopada 1986 r. w sprawie Gillow przeciwko Wielkiej Brytanii (seria A, nr 109, § 55).

103 — Wyrok ETPC z dnia 26 marca 1987 r. w sprawie Leander przeciwko Szwecji (seria A, nr 116, § 59).

104 — Zobacz np. wyrok ETPCz z dnia 6 września 1978 r. w sprawie Klass (seria A, nr 28, § 59) à propos tajnego monitorowania korespondencji i rozmów telefonicznych obywateli do celów walki z terroryzmem. W tym wyroku wyżej wymieniony Trybunał uznał za „należącą do istoty systemu konwencji pewną formę koncyliacji pomiędzy ważnymi względami obrony społeczeństwa demokratycznego a koniecznością ochrony praw jednostek".

105 — F. Sudre, „Droit européen et international des droits de l'homme", wydanie siódme poprawione, PUF, 2005, str. 219). Autor stwierdza także że „[w] zależności od bardziej lub mniej rygorystycznego powoływania przesłanki proporcjonalności — proporcje ścisłe, słuszne, rozsądne — Trybunał Praw Człowieka modyfikuje stopień sprawowanej kontroli, a w konsekwencji, a w konsekwencji zmienia szerokość marginesu uznania pozostawionego państwu [...]".

106 — Wyrok ETPC z dnia 25 lutego 1997 r. w sprawie Z. przeciwko Finlandii (*Recueil des arrêts et décisions* 1997-I).

wieka stoi na stanowisku, że margines uznania pozostawiony państwu jest wąski, a jego kontrola sądowa powinna być bardziej ścisła [107].

230. Natomiast jeśli cel ingerencji wiąże się z ochroną bezpieczeństwa państwa [108] lub też ze zwalczaniem terroryzmu [109], Europejski Trybunał Praw Człowieka skłania się ku pozostawieniu państwom szerokiego marginesu uznania.

231. Ze względu na istotę i znaczenie celu związanego ze zwalczaniem terroryzmu, który w ramach systemu PNR wydaje się przeważać, oraz z uwagi na politycznie delikatny kontekst, w jakim odbywały się rokowania między Wspólnotą a Stanami Zjednoczonymi, sądzę, że w niniejszej sprawie Trybunał powinien uznać, iż przy negocjowaniu z władzami amerykańskimi warunków systemu PNR Rada i Komisja dysponowały szerokim marginesem uznania. Co za tym idzie, w celu respektowania owego szerokiego marginesu uznania Trybunał powinien moim zdaniem ograniczyć zakres wykonywanej kontroli konieczności ingerencji do badania na okoliczność ewentualnego oczywistego błędu w ocenie [110]. Wykonując taką ograniczoną kontrolę Trybunał uniknąłby niebezpieczeństwa związanego z zastąpieniem jego własną oceną oceny dokonywanej przez polityczne organy wspólnotowe odnośnie do rodzaju środków najbardziej adekwatnych i dogodnych do zwal-

107 — Podobnie F. Sudre, op. cit., str. 219. Zobacz także P. Wachsmann, „Le droit au secret de la vie privée", w: S. Sudre S. (dir.), „Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme", Bruylant, 2005, str. 141: na temat przywołanego wyżej wyroku Z. przeciwko Finlandii, autor zauważa, że „[k]ontrola konieczności ingerencji w omawianej sprawie została wykonana bardzo dokładnie, co tłumaczy niezwykle drażliwy charakter kwestii ujawnienia osobom trzecim informacji o seropozytywności jakiejś osoby".

108 — Wyrok w sprawie Leander przeciwko Szwecji, cyt. wyżej. Torsten Leander został zatrudniony jako strażnik w muzeum marynarki w Szwecji, ale stracił pracę w wyniku kontroli kadrowej, przy której zebrano na jego temat tajne informacje. Na tej podstawie władze doszły do wniosku, że T. Leander nie może pracować w muzeum, którego magazyny znajdują się na terenach wojskowych objętych zakazem wstępu dla osób nieupoważnionych. Przy okazji tej sprawy Europejski Trybunał Praw Człowieka ustalił jasną zasadę, że rejestrowanie, podobnie jak udostępnianie danych osobowych w połączeniu z odmową przyznania prawa do odparcia zarzutów stanowi naruszenie prawa do poszanowania życia prywatnego. Przy ocenie uzasadnienia takiego naruszenia sędziowie Trybunału uznali, że „[w] celu ochrony bezpieczeństwa państwa układające się strony bezspornie potrzebują przepisów, które upoważniają właściwe organy krajowe do gromadzenia informacji o osobach oraz ich utrwalania w tajnych rejestrach, a następnie ich wykorzystywania do oceny przydatności kandydatów na stanowiska istotne z punktu widzenia wyżej wspomnianego bezpieczeństwa" (§ 59). Wziąwszy pod uwagę gwarancje, w jakie wyposażony był szwedzki system kontroli pracowników oraz szeroki margines swobody pozostawiony państwu, Trybunał orzekł, że „pozwany rząd miał prawo uznać, że interesy bezpieczeństwa państwa w tym przypadku były ważniejsze od interesów prywatnych skarżącego". Ingerencja, która dotknęła T. Leandra, nie była więc nieproporcjonalna w stosunku do zamierzonego uprawnionego celu (§ 67).

109 — Zobacz wyrok ETPC z dnia 28 października 1994 r. w sprawie Murray przeciwko Wielkiej Brytanii (seria A, nr 300-A, § 47 i 90). W tej sprawie zwalczanie terroryzmu pozwoliło usprawiedliwić zbieranie przez siły zbrojne informacji osobistych na temat pierwszej skarżącej. Trybunał podkreślił w szczególności, że nie jest jego rolą „zastępowanie własną oceną oceny władz krajowych co do wyboru najlepszej polityki w dziedzinie ścigania przestępstw terrorystycznych" (§ 90). Zobacz także ww. wyrok w sprawie Klass, § 49.

110 — Według D. Ritlenga, podobnie jak w przypadku synonimicznego pojęcia „oczywistego naruszenia", oczywisty błąd w ocenie zachodzi „w przypadku poważnego naruszenia przepisów prawa w takim stopniu, że jest ono oczywiste. Bez względu na swój dyskrecjonalny charakter, ocena faktów nie może prowadzić instytucji wspólnotowych do podejmowania dowolnych decyzji; poprzez kontrolę oczywistych błędów w ocenie sąd zakazuje korzystania ze swobody oceny w sposób poważnie naruszający jej zasady". Zobacz „Le contrôle de le légalité des actes communautaires par la Cour de justice et le Tribunal de première instance des Communautés européennes", praca obroniona w dniu 24 stycznia 1998 r. na Uniwersytecie Roberta Schumana w Strasburgu, str. 538, pkt 628.

czania terroryzmu i innych poważnych przestępstw.

232. W celu ustalenia zakresu kontroli, jaką zamierza przeprowadzić, Trybunał może oprzeć się — poza przywołanym powyżej orzecznictwem Europejskiego Trybunału Praw Człowieka — także na własnym orzecznictwie, ponieważ orzekał już, iż instytucja wspólnotowa w niektórych dziedzinach dysponuje szerokim marginesem uznania, „[...] jedynie oczywiście niewłaściwy charakter środka podjętego w tej dziedzinie w odniesieniu do celu, jaki realizują odpowiednie instytucje, może naruszyć ważność takiego środka" [111]. Ograniczenie kontroli proporcjonalności „jest szczególnie istotne", kiedy „Rada musi godzić rozbieżne interesy i podejmuje w ten sposób decyzje wiążące się z wyborami o charakterze politycznym, należące do jej kompetencji własnych" [112]. Ograniczenie kontroli może także uzasadniać okoliczność, iż w określonej dziedzinie instytucja wspólnotowa musi dokonywać globalnych ocen [113].

233. To orzecznictwo oraz racje, które za nim stoją, powinny — według mojej opinii — zostać uwzględnione w niniejszej sprawie, ponieważ w ramach opracowywania systemu PNR Rada i Komisja zostały postawione wobec wyborów politycznych wymagających godzenia rozbieżnych interesów i wobec konieczności dokonywania globalnych ocen [114]. Byłoby to zgodne z zasadą podziału władzy, która nakazuje Trybunałowi respektować kompetencje polityczne wspólnotowych organów ustawodawczych i administracyjnych, a w związku z tym nie przejmować ich roli przy dokonywaniu wyborów politycznych.

234. Po przedstawieniu powyższych uwag należy teraz dokładnie zbadać, czy przyjmując poszczególne akty będące elementami systemu PNR Rada i Komisja przekroczyły

111 — Zobacz w kwestiach z zakresu wspólnej polityki rolnej wyrok Trybunału z dnia 13 listopada 1990 r. w sprawie C-331/88 Fedesa i in., Rec. str. I-4023, pkt 14. Zobacz także w kwestiach z zakresu prawa antydumpingowego wyrok Sądu z dnia 5 czerwca 1996 r. w sprawie T-162/94 NMB Francja i in. przeciwko Komisji, Rec. str. II-427, pkt 70).

112 — Zobacz w kwestiach z zakresu wspólnej polityki rolnej wyrok Trybunału z dnia 5 października 1994 r. w sprawie C-280/93 Niemcy przeciwko Radzie, Rec. str. I-4973, pkt 91. To orzecznictwo rozciąga się także na inne dziedziny jak np. sprawy z zakresu polityki społecznej, w których Trybunał przyznał Radzie „szeroki zakres swobody uznania w dziedzinie [...], która wymaga od ustawodawcy wspólnotowego dokonywania wyborów polityki społecznej, w ramach której dokonuje się globalnych ocen" (ww. wyrok w sprawie Zjednoczone Królestwo przeciwko Radzie, pkt 58). Podkreślam także, że w kwestii publicznego dostępu do dokumentów instytucji wspólnotowych oraz w odniesieniu do zakresu sądowej kontroli zgodności z prawem decyzji odmownych, Trybunał przyznał Radzie szeroki zakres swobody uznania w przypadku decyzji odmownych uzasadnionych względami ochrony interesu publicznego w zakresie stosunków międzynarodowych lub względami ochrony interesu publicznego związanego z bezpieczeństwem publicznym — zobacz w szczególności w kwestiach związanych z walką z terroryzmem wyrok Sądu z dnia 26 kwietnia 2005 r. w sprawach połączonych T-110/03, T-150/03 i T-405/03 Sison przeciwko Radzie, Zb.Orz. str. II-1429, pkt 46 i 71–82).

113 — Poza ww. wyrokiem w sprawie Zjednoczone Królestwo przeciwko Radzie jest wiele przykładów uwzględnienia przez wspólnotowy wymiar sprawiedliwości globalnego charakteru ocen, których muszą dokonywać instytucje wspólnotowe — zobacz w szczególności w sprawach swobody przedsiębiorczości: wyrok z dnia 13 maja 1997 r. w sprawie C-233/94 Niemcy przeciwko Parlamentowi i Radzie, Rec. p. I-2405, pkt 55. Jako przykład uwzględnienia przez Sąd „globalnych ocen natury gospodarczej i społecznej", zobacz wyrok z dnia 13 września 1995 r. w sprawach połączonych T-244/93 i T-486/93 TWD przeciwko Komisji, Rec. str. II-2265, pkt 82.

114 — Na przykład Komisja dysponowała według mnie szerokim marginesem uznania do ustalenia, czy w szczególnym przypadku przekazywania danych PNR Stany Zjednoczone mogą zapewnić odpowiedni poziom ochrony danych osobowych.

ewidentnie granice swobody uznania obowiązujące ze względu na prawo do poszanowania życia prywatnego, a zwłaszcza prawo do ochrony danych osobowych pasażerów lotniczych, w świetle zamierzonego uprawnionego celu.

235. Przy tej ocenie szczególne znaczenie ma treść Zobowiązań CBP, ponieważ zawiera szczegółowe informacje na temat gwarancji związanych z systemem PNR. Zaznaczam w tym względzie, że moim zdaniem błędem byłoby uważać, iż Zobowiązania nie mają mocy wiążącej i zawierają postanowienia, które mogą być swobodnie zmieniane lub wypowiedziane przez władze amerykańskie.

236. W istocie Zobowiązania, które — przypominam — są załącznikiem do decyzji o odpowiedniej ochronie, stanowią jeden z elementów składowych systemu PNR i w związku z tym ich nieprzestrzeganie prowadziłoby do paraliżu całego systemu. Podkreślam także, że pkt 1 i 2 porozumienia uzależniają istnienie obowiązku przetwarzania danych PNR, spoczywającego na przewoźnikach lotniczych od ścisłej zgodności z decyzją o odpowiedniej ochronie i tylko „tak długo dopóki decyzja ma zastosowanie". Ponadto zgodnie z brzmieniem pkt 3 porozumienia CBP „stwierdza, że wprowadza w życie zobowiązania załączone" do wyżej wymienionej decyzji. Wreszcie artykuły 3, 4 i 5 decyzji o odpowiedniej ochronie określają środki, jakie będą podejmowane w razie naruszenia norm ochrony ujętych w Zobowiązaniach. Wśród tych środków przewidziano, że właściwe władze państw członkowskich mogą zawiesić przepływ danych do CBP oraz że w razie nieprzestrzegania podstawowych zasad niezbędnych dla zapewnienia odpowiedniego poziomu ochrony osób, który dotyczą dane, decyzja o odpowiedniej ochronie może być uchylona lub zawieszona, a w efekcie przestaną obowiązywać pkt 1 i 2 porozumienia.

237. Aby skłonić Trybunał do stwierdzenia, że ingerencja w życie prywatne tych pasażerów narusza zasadę proporcjonalności, Parlament w pierwszej kolejności powołał argument, że CBP żąda od linii lotniczych nadmiernie dużej liczby elementów danych. Ponadto uważa, że niektóre wymagane pozycje danych PNR mogą zawierać dane wrażliwe.

238. Uważam, że przy ustalaniu listy 34 elementów danych osobowych, załączonej do decyzji o odpowiedniej ochronie, Komisja nie zatwierdziła środka w oczywisty sposób nieadekwatnego dla osiągnięcia celu związanego ze zwalczaniem terroryzmu i innych poważnych przestępstw. Z jednej strony bowiem należy podkreślić znaczenie wywiadu w walce z terroryzmem, ponieważ uzyskanie odpowiednich informacji może pozwolić służbom bezpieczeństwa danego państwa zapobiec ewentualnemu zamachowi terrorystycznemu — w takiej sytuacji ze względu konieczność opracowania profilu potencjalnych terrorystów można wymagać dużej ilości danych; z drugiej zaś strony

okoliczność, iż inne akty prawne związane z wymianą informacji obowiązujące w Unii Europejskiej przewidują udostępnianie mniejszej liczby danych, nie wystarcza, by wykazać nadmierny charakter liczby danych wymaganych przez szczególny instrument przeznaczony do walki z terroryzmem, jakim jest system PNR [115].

239. Ponadto chociaż słuszna jest uwaga Parlamentu, że trzy wymagane pozycje danych mogą zawierać tzw. dane wrażliwe [116], zaznaczam jednak, że z jednej strony dostęp CBP do tych pozycji został ściśle ograniczony na podstawie ust. 5 Zobowiązań, z drugiej zaś strony na mocy ust. 9–11 Zobowiązań jest wykluczone, by CBP mogło wykorzystywać dane wrażliwe, a ponadto system filtrujący takie dane został wprowadzony przez CBP, zgodnie ze zobowiązaniem podjętym przez to biuro [117].

240. Po drugie Parlament uważa, że dane PNR pasażerów są przechowywane przez władze amerykańskie przez okres zbyt długi w stosunku do zamierzonego celu.

241. Okres przechowywania danych został określony w ust. 15 Zobowiązań, który przewiduje, że co do zasady dostęp on-line do tych danych dla uprawnionych użytkowników w CBP jest początkowo możliwy przez okres siedmiu dni. Po jego upływie możliwość wglądu do danych będzie miała ograniczona liczba uprawnionych urzędników przez okres trzech lat i sześciu miesięcy. Wreszcie po upływie tego kolejnego okresu dane, do których w tym czasie nie próbowano uzyskać dostępu ręcznie, zostaną zniszczone, natomiast dane, do których uzyskano ręcznie dostęp w okresie trzech lat i sześciu miesięcy, zostaną przekazane przez CBP do pliku skasowanych danych, gdzie pozostaną przez okres ośmiu lat przed ich całkowitym zniszczeniem [118].

242. Z tego postanowienia wynika, że normalny okres przechowywania danych pochodzących z PNR wynosi trzy lata i sześć miesięcy, z wyjątkiem danych, do których w tym czasie uzyskano ręcznie dostęp. W moim mniemaniu nie jest to okres nadmiernie długi, zwłaszcza biorąc pod uwagę fakt, iż — jak wskazuje Rada — śledztwa prowadzone w związku z zamachami terrorystycznymi lub innymi poważnymi przestępstwami mogą trwać niekiedy

115 — Według Komisji „system PNR wprowadza specyficzne rozwiązanie dla specyficznego problemu [...]. W istocie Wspólnota i Stany Zjednoczone uzgodniły zamknięty system ochrony danych specjalnie dla CBP, odrębny od systemu amerykańskiego, obwarowany dodatkowymi gwarancjami administracyjnymi w postaci kontroli amerykańskiej oraz administracyjnej i prawnej kontroli po stronie europejskiej", pkt 13 uwag Komisji do uwag złożonych przez EIOD jako interwenienta w sprawie C-318/04).

116 — Przypominam, że chodzi o pozycje o numerach: 19 — „Uwagi ogólne"; 26 — „Informacja OSI (inn[e] usług[i])" oraz 27 — „Informacja SSI/SSR (specjalne usługi)".

117 — Zobacz pkt 20 i 21 uwag Komisji do uwag interwenienta złożonych przez EIOD w sprawie C-318/04.

118 — Wyjaśniono również, w przypisie 7 do Zobowiązań, że kiedy rejestr PNR jest przesyłany do pliku skasowanego rejestru, jest przechowywany w postaci pierwotnej, a nie w postaci gotowych formularzy do wyszukania, a więc nie może być wykorzystywany w „tradycyjnych" śledztwach.

wiele lat. Toteż mimo iż co do zasady wskazane jest, by dane osobowe były przechowywane przez krótki okres, w niniejszej sprawie należy rozpatrywać długość okresu przechowywania danych pochodzących z PNR mając na uwadze ich przydatność nie tylko do celów zapobiegania terroryzmowi, ale szerzej do zwalczania przestępczości.

1 – 243. W świetle powyższych uwag zasady przechowywania danych określone w ust. 15 Zobowiązań według mojej oceny nie stanowią oczywistego naruszenia prawa do poszanowania życia prywatnego.

244. Po trzecie Parlament zarzuca systemowi PNR, że nie przewidziano w nim kontroli sądowej w odniesieniu do przetwarzania danych osobowych przez władze amerykańskie.

245. Nadmieniam, że zarówno konwencja nr 108, jak i dyrektywa 95/46, przewidują możliwość wystąpienia na drogę sądową w razie naruszenia przepisów prawa krajowego wprowadzających w życie zasady określone w tych dwóch aktach prawnych [119].

119 — Zobacz art. 8 lit. d) i art. 10 konwencji nr 108, a także art. 22 dyrektywy 95/46.

246. W świetle art. 8 ust. 2 EKPC, według mojej oceny, zasady określone w ust. 36 i następnych Zobowiązań przewidujące szereg gwarancji w zakresie informowania, dostępu do danych i środków odwoławczych przysługujących pasażerom lotniczym, których dotyczą dane, pozwalają uniknąć ewentualnych nadużyć. Całość tych gwarancji prowadzi mnie do wniosku, iż wziąwszy pod uwagę szeroki margines uznania, który — moim zdaniem — powinno się w tym przypadku przyznać Radzie i Komisji, ingerencja w życie prywatne pasażerów lotniczych jest proporcjonalna do uprawnionego celu, któremu służy system PNR.

247. Dokładniej rzecz ujmując, należy zaznaczyć, że poza informacjami ogólnymi, które CBP zobowiązuje się udzielać pasażerom lotniczym [120], ust. 37 Zobowiązań przewiduje, że osoby, których dane dotyczą, zgodnie z ustawą o wolności informacji [121], mogą otrzymać kopię danych zawartych

120 — Zobacz ust. 36 Zobowiązań, który stanowi:
„CBP będzie udzielać informacji podróżującym na temat wymogów dotyczących PNR oraz kwestii związanych z ich wykorzystaniem (np. ogólnych informacji dotyczących organu, z upoważnienia którego dane są zbierane, celu zbierania danych, ochrony danych, przekazywania danych, tożsamości urzędnika odpowiedzialnego, dostępnych środków odwoławczych oraz informacji kontaktowych dla osób mających pytania lub zgłaszających ewentualne problemy itp., poprzez zamieszczenie na stronie internetowej CBP, ulotkach dla podróżnych itp.)".

121 — Chodzi o „Freedom of Information Act" (tytuł 5, sekcja 552 United States Code, zwany dalej „FOIA"). W sprawie dokumentów posiadanych przez CBP należy zapoznać się z przepisami FOIA w związku z przepisami tytułu 19 sekcja 103.0 i nast. Code of Federal Regulations.

w PNR znajdujących się w bazie danych CBP, odnoszących się do wnioskodawcy [122].

248. Wprawdzie ust. 38 Zobowiązań przewiduje możliwość, „[w] określonych wyjątkowych okolicznościach", odrzucenia lub odroczenia ujawnienia przez CBP całej (lub częściej fragmentu) zawartości PNR, np. jeżeli ujawnienie „mogłoby zakłócać postępowanie wykonawcze" lub jeśli „ujawniłoby techniki i procedury działań organów ścigania", jednak niezależnie od faktu, iż korzystanie z tego uprawnienia przez CBP jest dokładnie określone ustawą, należy zaznaczyć, że ten sam ustęp Zobowiązań przewiduje, że „zgodnie z FOIA, każdy wnioskodawca ma prawo do *administracyjnego i sądowego zakwestionowania* decyzji CBP w sprawie wstrzymania ujawnienia informacji" [123].

249. Ponadto jeśli chodzi o wnioski o sprostowanie danych PNR zawartych w bazie danych CBP oraz skargi osób fizycznych w sprawie przetwarzania ich danych PNR przez CBP, ust. 40 Zobowiązań ustala, że powinny być składane do „Assistant Commissioner" CBP [124].

250. W sytuacji gdy CBP nie jest w stanie rozstrzygnąć skargi, należy ją skierować do „Głównego Urzędnika ds. Prywatności w Departamencie Bezpieczeństwa Wewnętrznego" („Chief Privacy Officer") [125].

251. Równocześnie w postanowieniach ust. 42 Zobowiązań przewidziano, że „Biuro ds. Prywatności Ministerstwa Bezpieczeństwa Wewnętrznego będzie rozpatrywać w trybie przyśpieszonym skargi skierowane do niego przez OOD państw członkowskich UE w imieniu osoby zamieszkującej w UE w zakresie, w jakim osoba ta upoważniła OOD do działania w jej imieniu i która twierdzi, że jej skarga w sprawie ochrony danych zawartych w PNR nie została rozpatrzona w zadowalający sposób przez CBP (jak ustanowione w ust. 37–41 niniejszych Zobowiązań) lub Biuro ds. Prywatności Ministerstwa Bezpieczeństwa Wewnętrznego".

122 — FOIA wprowadza domniemanie, że każdy federalny dokument rządowy powinien być udostępniony każdej osobie. Jednakże instytucja rządowa może być zwolniona z obowiązku ujawnienia wynikającego z tego domniemania, jeśli udowodni, że dane informacje zaliczają się do kategorii wyłączonych spod obowiązku ujawniania. Przy czym należy zaznaczyć, że zgodnie z ust. 37 Zobowiązań „[w] przypadku wniosku złożonego przez osobę, której dane dotyczą, fakt, że CBP w innych przypadkach traktuje dane zawarte w PNR jako poufne informacje osobowe oraz poufne informacje handlowe przewoźnika lotniczego, nie będzie wykorzystany przez CBP jako podstawa zgodnie z FOIA do wstrzymania się od ujawnienia danych zawartych w PNR osobie, której te dane dotyczą".

123 — Podkreślenie moje. Ustęp 38 Zobowiązań odsyła w tym zakresie do przepisów zawartych w tytule 5 United States Code, sekcja 552(a)(4)(B) oraz w tytule 19 Code of Federal Regulations, sekcje 103.7–103.9. Z aktów tych wynika, że odwołanie się na drodze sądowej („judicial review") od decyzji CBP oddalającej wniosek o ujawnienie powinno być poprzedzone odwołaniem w trybie administracyjnym do FOIA Appeals Officer (tytuł 19 sekcja 103.7 Code of Federal Regulations). Jeśli odmowa ujawnienia zostanie utrzymana w mocy w odwoławczym postępowaniu administracyjnym, wnioskodawca może wówczas wystąpić na drogę sądową do federalnego District Court, który jest właściwy do zarządzenia ujawnienia wszelkich informacji bezzasadnie odmówionych przez organ rządowy.

124 — Adres „Assistant Commissioner" jest wskazany w tym samym ustępie.

125 — Jego adres figuruje w ust. 41 Zobowiązań.

252. Ustęp 42 przewiduje również z jednej strony, że wyżej wymienione biuro „przekaże swoje wnioski i doradzi właściwemu OOD w sprawie działań, jakie należy podjąć, jeżeli zachodzi taka potrzeba", a równocześnie Chief Privacy Officer „zawrze w swoim sprawozdaniu dla Kongresu kwestie związane z liczbą, treścią i rozpatrzeniem skarg dotyczących przetwarzania danych osobowych, takich jak zawarte w PNR zawrze w swoim sprawozdaniu dla Kongresu kwestie związane z liczbą, treścią i rozpatrzeniem skarg dotyczących przetwarzania danych osobowych, takich jak zawarte w PNR" [126].

253. Parlament słusznie zauważył, że Chief Privacy Officer nie jest organem sądowym. Jednakże należy zaznaczyć, że mamy tu do czynienia z organem administracyjnym w pewnym stopniu niezależnym od Ministerstwa Bezpieczeństwa Wewnętrznego, a jego decyzje są wiążące [127].

254. W rezultacie możliwość składania w takim trybie przez pasażerów lotniczych skargi do Chief Privacy Officer oraz skorzystania z sądowego środka odwoławczego przysługującego w ramach FOIA stanowią poważne gwarancje dla ich prawa do poszanowania życia prywatnego. Z racji tych gwarancji uważam, że Rada i Komisja nie przekroczyły granic swobody uznania obowiązujących je przy ustanawianiu systemu PNR.

255. Ostatni argument zgłoszony przez Parlament zarzuca systemowi PNR, że wykracza poza granice tego, co konieczne do walki z terroryzmem i innymi poważnymi przestępstwami, gdyż pozwala na przekazywanie danych pasażerów lotniczych innym organom publicznym. Według Parlamentu CBP dysponuje uprawnieniem dyskrecjonalnym do przekazywania danych pochodzących z PNR innym władzom publicznym, w tym także organom rządowym innych państw, co jest sprzeczne z art. 8 ust. 2 EKPC.

256. Nie podzielam tej opinii. W istocie również w tym zakresie gwarancje, jakimi obwarowano przepływ danych PNR do innych organów rządowych, pozwalają moim zdaniem uważać, że ingerencja w życie prywatne pasażerów lotniczych jest proporcjonalna w stosunku do celu, któremu służy system PNR.

257. Nawet jeśli Zobowiązania pozostawiają CBP znaczny zakres uznania, zwracam jed-

126 — Zobacz podobnie ust. 5 sekcji 222 amerykańskiej ustawy z 2002 r. o bezpieczeństwie wewnętrznym (Homeland Security Act — Public Law, 107–296, z dnia 25 listopada 2002 r.), która przewiduje, że Chief Privacy Officer ma obowiązek składać każdego roku Kongresowi sprawozdanie na temat działań Ministerstwa Bezpieczeństwa Wewnętrznego mających wpływ na ochronę prywatności oraz ewentualnych skarg na naruszenia prywatności.

127 — Zobacz przypis 11 Zobowiązań, z którego wynika, że Chief Privacy Officer „jest niezależny od wszystkich dyrekcji Ministerstwa Bezpieczeństwa Wewnętrznego. Jest statutowo zobowiązany do zapewnienia, że informacje osobowe wykorzystywane są w sposób zgodny z właściwym ustawodawstwem [...]. Ustalenia [głównego urzędnika] są wiążące dla ministerstwa i nie mogą być podważone na podstawie kwestii politycznych". Dodam też, że wymóg dotyczący możliwości wniesienia środka odwoławczego do niezależnego organu posiadającego kompetencje decyzyjne wynika m.in. z wyroku Europejskiego Trybunału Praw Człowieka z dnia 7 lipca 1989 r., Gaskin przeciwko Wielkiej Brytanii (seria A, nr, 160, § 49). Nadmieniam także, iż art. 8 Karty praw podstawowych Unii w ust. 3 przewiduje, że przestrzeganie zasad, które ustanawia „podlega kontroli niezależnego organu".

nak uwagę, że uznanie to podlega ograniczeniom. Otóż zgodnie z ust. 29 Zobowiązań, dostarczanie danych PNR innym organom rządowym „odpowiedzialnymi za walkę z terroryzmem lub ściganie przestępstw" „włącznie z zagranicznymi" może się odbywać tylko „na zasadzie jednostkowych przypadków" oraz wyłącznie co do zasady „do celów zapobiegania i zwalczania przestępstw wymienionych w ust. 3 niniejszego dokumentu". CBP, zgodnie z ust. 30 Zobowiązań, powinno ustalić, czy powód do ujawnienia danych zawartych w PNR innemu organowi mieści się w ramach wymienionych celów.

258. Wprawdzie ust. 34 i 35 Zobowiązań rozszerzają niejako listę tego rodzaju celów, gdyż skutkują umożliwieniem, odpowiednio, po pierwsze wykorzystania lub ujawnienia danych PNR właściwym organom rządowym, „jeżeli jest to konieczne w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innych osób, w szczególności w odniesieniu do znacznego zagrożenia zdrowia", a po drugie umożliwieniem wykorzystania lub ujawnienia danych PNR „w postępowaniach karnych oraz w innych przypadkach wymaganych przez prawo".

259. Natomiast niezależnie od tego, że cele te są w większości związane z uprawnionym celem, któremu służy system PNR, zwracam uwagę, że Zobowiązania zawierają pewną liczbę gwarancji. Na przykład ich ust. 31 przewiduje, że „[d]o celów uregulowania upowszechniania danych zawartych w PNR, które mogą być przekazywane innym wyznaczonym organom, CBP jest traktowane jako »właściciel« danych i »wyznaczone organy« są zobowiązane na mocy wyżej wymienionych warunków" do wypełnienia wielu obowiązków. Między innymi na organach będących odbiorcami danych ciąży obowiązek „zapewnienia uporządkowanego trybu pozbywania się informacji zawartych w PNR, które zostały otrzymane, zgodnie z procedurami przechowywania danych w rejestrach wyznaczonych organów" oraz „otrzymania wyraźnej zgody CBP do dalszego ich upowszechniania".

260. Dodatkowo ust. 32 Zobowiązań precyzuje, że „[k]ażde ujawnienie przez CBP danych zawartych w PNR będzie uwarunkowane od traktowania ich przez agencję otrzymującą je jako poufnej informacji handlowej, prawnie chronionej, jako poufnych informacji osobowych [...], które powinny być traktowane jako wyłączone z ujawniania zgodnie z ustawą o wolności informacji [...]". W dalszej części ten sam ustęp wskazuje, że „agencja otrzymująca informacje otrzyma także informacje, że dalsze ujawnianie tych informacji jest niedozwolone bez wcześniejszego otrzymania wyraźnej zgody od CBP", które nie zezwala na „na dalsze przekazywanie danych zawartych w PNR do celów innych niż określone w ust. 29, 34 i 35 niniejszego dokumentu". Wreszcie ust. 33 Zobowiązań stanowi, że „[o]soby zatrudnione przez wyznaczony organ, które bez otrzymania odpowiedniego zezwolenia ujawniły dane zawarte w PNR, mogą podlegać sankcjom karnym".

261. Wzięcie pod uwagę wszystkich tych gwarancji wyklucza moim zdaniem możliwość uznania, że Rada i Komisja przekroczyły granice szerokiego marginesu uznania, jaki — według mojej opinii — należy im pozostawić do celów zwalczania terroryzmu i innych poważnych przestępstw.

262. Wynika stąd, że zarzuty oparte na naruszeniu prawa do ochrony danych osobowych oraz na naruszeniu zasady proporcjonalności są bezzasadne i w związku z tym powinny zostać oddalone.

D — *W przedmiocie zarzutu opartego na braku wystarczającego uzasadnienia decyzji Rady*

263. Parlament utrzymuje, że decyzja Rady nie spełnia wymogu uzasadnienia wynikającego z art. 253 WE. W szczególności Parlament formułuje względem tej decyzji zarzut, że nie zawiera ona żadnego uzasadnienia, które by wyjaśniało, czy oraz w jakim zakresie przedmiot tego aktu wiąże się z funkcjonowaniem rynku wewnętrznego.

264. Natomiast Rada, popierana przez Zjednoczone Królestwo i Komisję, stoi na stanowisku, że uzasadnienie jej decyzji jest zgodne z wymogami ustalonymi przez Trybunał.

265. Uważam, że mimo swojej zwięzłości uzasadnienie decyzji Rady jest wystarczające.

266. Zgodnie z utrwalonym orzecznictwem Trybunału uzasadnienie wymagane przez przepis art. 253 WE „powinno być dostosowane do charakteru konkretnego aktu, ukazywać jasno i jednoznacznie tok rozumowania instytucji, która jest jego autorem, w sposób umożliwiający zainteresowanym poznanie motywów przyjęcia środka, a Trybunałowi sprawowanie kontroli". Z tego orzecznictwa wynika ponadto, że „nie jest wymagane, by w uzasadnieniu były wyszczególnione wszystkie istotne elementy stanu faktycznego i prawnego, ponieważ w celu rozstrzygnięcia kwestii, czy uzasadnienie aktu spełnia wymogi [art. 253 WE], należy je oceniać nie pod względem treści, lecz także kontekstu oraz całości przepisów prawnych regulujących daną dziedzinę" [128].

267. Co do charakteru aktu należy przypomnieć, że mamy tu do czynienia z decyzją, której głównym celem jest zatwierdzenie w imieniu Wspólnoty porozumienia miedzy nią a Stanami Zjednoczonymi. Decyzja zawiera w tym względzie niezbędne informacje na temat trybu postępowania, tj. przyjęcia przez Radę zgodnie z procedurą określoną w art. 300 ust. 2 akapit pierwszy WE, a także

128 — Zobacz np. wyrok z dnia 29 lutego 1996 r. w sprawie C-56/93 Belgia przeciwko Komisji, Rec. str. I-723, pkt 86.

informację o tym, że Parlament nie wydał opinii w terminie ustalonym przez Radę na podstawie art. 300 ust. 3 akapit pierwszy WE. Ponadto zwracam uwagę, że w preambule decyzja Rady odwołuje się do art. 95 WE.

268. Ponadto wziąwszy pod uwagę szczególny charakter omawianej decyzji, trudno ją całkowicie oddzielić od umowy międzynarodowej, której dotyczy, dlatego też badanie, czy jej uzasadnienie jest wystarczające, powinno — w moim mniemaniu — obejmować również preambułę samego porozumienia. Lektura decyzji Rady w zestawieniu z preambułą porozumienia umożliwia Trybunałowi wykonanie kontroli, jak to wykazało badanie poprzednich zarzutów, w szczególności w zakresie ustalenia, czy wybór podstawy prawnej był właściwy.

269. W związku z powyższym uważam, że zarzut niedostatecznego uzasadnienia decyzji Rady jest bezzasadny i powinien zostać oddalony.

E — *W przedmiocie zarzutu opartego na naruszeniu zasady lojalnej współpracy, o której mowa w art. 10 WE*

270. W tym zarzucie Parlament twierdzi, że nawet jeśli art. 300 ust. 3 akapit pierwszy WE pozwala Radzie wyznaczyć mu termin wydania opinii stosownie do pilności sprawy, a wszczęcie postępowania w celu uprzedniego uzyskania opinii Trybunału, o której mowa w art. 300 ust. 6 WE, nie ma charakteru zawieszającego, Rada w ramach procedury zawierania porozumienia naruszyła obowiązek lojalnej współpracy, jaki na nią nakłada art. 10 WE.

271. Rada, popierana przez Komisję i Zjednoczone Królestwo, twierdzi z kolei, że nie naruszyła zasady lojalnej współpracy zawierając porozumienie, mimo iż Parlament wystąpił do Trybunału z wnioskiem o wydanie opinii w trybie art. 300 ust. 6 WE.

272. Artykuł 10 WE nakłada na państwa członkowskie obowiązek lojalnej współpracy z instytucjami wspólnotowymi, ale nie sankcjonuje wprost zasady lojalnej współpracy między samymi instytucjami. Jednakże Trybunał uznał, że w ramach dialogu międzyinstytucjonalnego, na którym opiera się w szczególności procedura konsultacji, obowiązują takie same wzajemne zasady lojalnej współpracy, jak te panujące w stosunkach pomiędzy państwami członkowskimi a instytucjami wspólnotowymi" [129].

129 — Wyroki z dnia 27 września 1988 r. w sprawie 204/86 Grecja przeciwko Radzie, Rec. str. 5323, pkt 16, oraz z dnia 30 marca 1995 r. w sprawie C-65/93 Parlament przeciwko Radzie, Rec. str. I-643, pkt 23.

273. Z okoliczności faktycznych niniejszej sprawy wynika, że w dniu 17 marca 2004 r. Komisja przekazała Parlamentowi projekt decyzji Rady, a następnie pismem z dnia 25 marca 2004 r. zwróciła się do Parlamentu o wydanie opinii na temat tego projektu najpóźniej do dnia 22 kwietnia 2004 r. W swoim piśmie Rada podkreśliła, że „[w]alka z terroryzmem, uzasadniająca projektowane postanowienia, stanowi jeden z podstawowych priorytetów Unii Europejskiej. W chwili obecnej przewoźnicy lotniczy oraz pasażerowie znajdują się w sytuacji niepewności, którą należy pilnie zakończyć. Dodatkowo należy chronić interesy finansowe podmiotów, których sprawa dotyczy".

274. W dniu 21 kwietnia 2004 r. Parlament postanowił wystąpić, zgodnie z art. 300 ust. 6 WE, do Trybunału o wydanie opinii w przedmiocie zgodności projektowanej umowy z postanowieniami traktatu.

275. W dniu 28 kwietnia 2004 r. Rada, na podstawie art. 300 ust. 3 akapit pierwszy WE, wystosowała do Parlamentu pismo, w którym zwróciła się do niego o wydanie opinii dotyczącej zawarcia umowy w terminie do dnia 5 maja 2004 r. Na uzasadnienie pilności sprawy powtórzyła argumenty zawarte w piśmie z dnia 25 marca 2004 r.

276. Wniosek Rady o rozpatrzenie w trybie pilnym został odrzucony przez Parlament, którego przewodniczący równocześnie zwrócił się do Rady i Komisji, by powstrzymały się z realizacją swych zamierzeń do czasu wydania przez Trybunał opinii, o którą Parlament wystąpił w dniu 21 kwietnia 2004 r. Mimo wszystko Rada w dniu 17 maja 2004 r. wydała zaskarżoną decyzję.

277. W moim mniemaniu Rada nie naruszyła obowiązku lojalnej współpracy w stosunku do Parlamentu przez przyjęcie decyzji zatwierdzającej porozumienie w imieniu Wspólnoty przed zakończeniem postępowania z wniosku o wydanie opinii Trybunału wszczętego przez Parlament na podstawie art. 300 ust. 6 WE.

278. W istocie — jak zresztą przyznaje sam Parlament — wszczęcie postępowania z wniosku o wydanie opinii przez Trybunał nie ma skutku zawieszającego. Zatem nie stanowi dla Rady przeszkody do wydania decyzji zatwierdzającej umowę, chociaż postępowanie wciąż jeszcze jest w toku i mimo iż okres pomiędzy złożeniem wniosku o opinię Trybunału a wydaniem decyzji zatwierdzającej umowę jest, jak w przypadku rozpoznawanej sprawy, stosunkowo krótki.

279. Wypada w tym miejscu zaznaczyć, że brak charakteru zawieszającego wniosku o wydanie opinii Trybunału wniesionego na podstawie art. 300 ust. 6 WE można wywieść zarówno z brzmienia tego artykułu, który nie mówi o nim wyraźne, jak również z orzecznictwa Trybunału. Stwierdził on bowiem

w opinii 3/94 [130], że wniosek o opinię staje się bezprzedmiotowy i że nie ma potrzeby, by Trybunał się do niego ustosunkowywał, jeżeli przedmiotowa umowa, która w momencie złożenia wniosku była umową projektowaną, w międzyczasie została zawarta. Dodał również, że z jednej strony postępowanie z art. 300 ust. 6 WE „ma po pierwsze na celu [...] zapobiec trudnościom wynikającym z niezgodności z traktatem umów międzynarodowych tworzących zobowiązania po stronie Wspólnoty, a nie *chronić interesy i prawa państwa członkowskiego lub instytucji wspólnotowej, która wystąpiła o wydanie opinii*" [131], z drugiej zaś strony „[w] każdym stanie rzeczy państwu lub instytucji wspólnotowej, które występowały z wnioskiem o wydanie opinii, służy skarga o stwierdzenie nieważności decyzji Rady o zawarciu umowy [...]". [132].

280. Ponadto z akt sprawy oraz z motywu drugiego decyzji Rady wynika, że Rada wystarczająco uzasadniła pilny charakter sprawy, na który powoływała się w celu uzyskania opinii Parlamentu w krótkim terminie, zgodnie z art. 300 ust. 3 akapit pierwszy WE. Na koniec zwracam uwagę, iż tenże artykuł wyraźnie przewiduje, że „[w] przypadku braku opinii w tym terminie Rada może stanowić samodzielnie".

130 — Opinia z dnia 13 grudnia 1995 r., Rec. str. I-4577, wydana na wniosek Republiki Federalnej Niemiec w przedmiocie zgodności z traktatem umowy ramowej dotyczącej bananów pomiędzy Wspólnotą Europejską a Kolumbią, Kostaryką i Wenezuelą.

131 — Punkt 21 opinii (podkreślenie moje).

132 — Punkt 22 opinii.

281. Zważywszy na wszystkie powyższe okoliczności, uważam, że zarzut oparty na naruszeniu przez Radę obowiązku lojalnej współpracy jest bezzasadny i powinien zostać oddalony.

VII — W przedmiocie kosztów

282. W sprawie C-318/04, w związku zasadnością skargi wniesionej przez Parlament, kosztami należy obciążyć Komisję, zgodnie z przepisami art. 69 § 2 regulaminu Trybunału. Ponadto na podstawie art. 69 § 4 regulaminu interwenienci tj. Zjednoczone Królestwo oraz EIOD, pokrywają własne koszty.

283. W sprawie C-317/04, w związku zasadnością skargi wniesionej przez Parlament, kosztami należy obciążyć Radę, zgodnie z przepisami art. 69 § 2 regulaminu Trybunału. Ponadto na podstawie art. 69 § 4 regulaminu interwenienci tj. Zjednoczone Królestwo, Komisja oraz EIOD, pokrywają własne koszty.

VIII — Wnioski

284. W świetle całości powyższych stwierdzeń proponuję Trybunałowi:

— w sprawie C-318/04 — stwierdzenie nieważności decyzji 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 Ceł i Ochrony Granic Stanów Zjednoczonych Ameryki;

— w sprawie C-317/04 — stwierdzenie nieważności decyzji Rady 2004/496/WE z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Ceł i Ochrony Granic.