I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa

(2008/C 110/01)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 286,

uwzględniając Kartę Praw Podstawowych Unii Europejskiej, w szczególności jej art. 8,

uwzględniając dyrektywę 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 ([1]),

uwzględniając rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych ([2]), w szczególności jego art. 41,

uwzględniając wniosek o wydanie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001, otrzymany od Komisji Europejskiej w dniu 13 listopada 2007 r.,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

I. WSTĘP

Konsultacje z Europejskim Inspektorem Ochrony Danych

1. Projekt wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa (zwany dalej „wnioskiem") został przesłany EIOD przez Komisję do zaopiniowania zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001.

2. Wniosek dotyczy przetwarzania danych PNR w obrębie UE i jest ściśle powiązany z innymi systemami gromadzenia i wykorzystywania danych dotyczących pasażera, zwłaszcza z umową z lipca 2007 roku między UE a USA. Systemy te cieszą się wielkim zainteresowaniem EIOD, który miał już okazję przesłać pewne wstępne uwagi w związku z przygotowanym przez Komisję kwestionariuszem dotyczącym planowanego unijnego systemu PNR rozesłanym głównym zainteresowanym stronom ([3]) w grudniu 2006 roku. EIOD z zadowoleniem przyjmuje wniosek Komisji o przeprowadzenie konsultacji. Jego zdaniem niniejsza opinia powinna zostać ujęta w preambule decyzji Rady.

Kontekst wniosku

3. Celem wniosku jest harmonizacja w państwach członkowskich przepisów zobowiązujących przewoźników lotniczych obsługujących loty z lub na terytorium przynajmniej jednego państwa członkowskiego do przekazywania danych PNR właściwym organom w celu zapobiegania przestępstwom terrorystycznym i międzynarodowej przestępczości zorganizowanej oraz ich zwalczania.

4. Unia Europejska zawarła z USA i z Kanadą umowy dotyczące przekazywania danych PNR do porównywalnych celów. Pierwsza umowa zawarta z USA w maju

([1]) Dz.U. L 281 z 23.11.1995, str. 31.
([2]) Dz.U. L 8 z 12.1.2001, str. 1.

([3]) W tym państwom członkowskim, organom ochrony danych i stowarzyszeniom linii lotniczych. Kwestionariusz został przygotowany, mając na względzie opracowanie przez Komisję Europejską oceny skutków omawianego wniosku.

2004 roku została zastąpiona nową w lipcu 2007 roku ([1]). Podobną umowę zawarto z Kanadą w lipcu 2005 r. ([2]) Ponadto mają się rozpocząć negocjacje między UE a Australią dotyczące umowy o wymianie danych PNR; również Korea Południowa wymaga danych PNR dotyczących lotów kończących się na jej terytorium, jak dotąd bez planu negocjacji na poziomie europejskim.

5. W obrębie UE wniosek ma uzupełnić dyrektywę Rady 2004/82/WE ([3]) w sprawie zobowiązania przewoźników do przekazywania danych pasażerów, zwanych danymi API, w celu zwalczania nielegalnej imigracji i usprawnienia kontroli granicznej. Dyrektywa ta powinna była zostać przetransponowana do prawodawstwa krajowego państw członkowskich najpóźniej do dnia 5 września 2006 r. Nie wszystkie państwa członkowskie jednak zapewniły jej wdrożenie.

6. W odróżnieniu od danych pasażera przekazanych przed podróżą (API), które mają umożliwić identyfikację poszczególnych osób, data PNR określone we wniosku mogłyby się przyczynić do oceny zagrożenia związanego z danymi osobami, uzyskiwania danych wywiadowczych i określania związków między osobami znanymi i nieznanymi.

7. Wniosek obejmuje następujące istotne elementy:

   — umożliwia udostępnianie przez przewoźników lotniczych danych PNR właściwym organom państw członkowskich w celu zapobiegania przestępstwom terrorystycznym i przestępczości zorganizowanej oraz ich zwalczania,

   — przewiduje wyznaczenie — z zasady w każdym państwie członkowskim — biur danych pasażerów (ang. *Passenger Information Unit* — PIU) odpowiedzialnych za gromadzenie danych PNR od przewoźników lotniczych (lub wyznaczonych pośredników) i przeprowadzanie oceny zagrożenia ze strony pasażerów,

   — odpowiednio ocenione informacje będą przekazywane właściwym organom każdego państwa członkowskiego. Informacje te będą podlegać wymianie z innymi państwami członkowskimi w zależności od przypadku i w wyżej określonych celach,

   — przekazywanie danych państwom spoza Unii Europejskiej jest obwarowane dodatkowymi warunkami,

   — dane będą przechowywane przez trzynaście lat, z tego osiem w archiwalnej bazie danych,

   — przetwarzanie danych ma podlegać (projektowi) decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (zwanej dalej „decyzją ramową o ochronie danych") ([4]),

   — komitet złożony z przedstawicieli państw członkowskich będzie wspierać Komisję w kwestiach związanych z protokołem i szyfrowaniem, a także kryteriami oceny zagrożenia i jej przeprowadzaniem,

   — przegląd decyzji ma nastąpić po trzech latach od jej wejścia w życie.

Punkt widzenia przyjęty w opinii

8. Wniosek, co do którego zasięgnięto opinii EIOD, stanowi kolejny krok na drodze do rutynowego gromadzenia danych o osobach, które w zasadzie nie są podejrzewane o popełnienie żadnego przestępstwa. Jak już wspomniano, ewolucja ta zachodzi na szczeblu europejskim i międzynarodowym.

9. EIOD odnotowuje także wspólną opinię Grupy Roboczej art. 29 i Grupy Roboczej ds. Policji i Wymiaru Sprawiedliwości w sprawie omawianego wniosku ([5]). EIOD zgadza się z tą opinią. Niniejsza opinia podkreśla i rozwija pewne dodatkowe zagadnienia.

10. Choć w swej opinii EIOD przeanalizuje wszystkie istotne aspekty wniosku, skupi się na czterech głównych kwestiach:

    — pierwsza z nich to zgodność planowanych środków z prawem. Kwestia celu, konieczności i proporcjonalności wniosku zostanie oceniona zgodnie z kryteriami określonymi w art. 8 Karty Praw Podstawowych Unii Europejskiej,

    — w opinii przeanalizowana zostanie kwestia prawa właściwego dla proponowanych operacji przetwarzania danych. Szczególnej uwagi wymaga zwłaszcza zakres zastosowania decyzji ramowej o ochronie danych w związku ze stosowaniem prawodawstwa dotyczącego ochrony danych w ramach pierwszego filaru. Poddane analizie zostaną również konsekwencje mającego zastosowanie systemu ochrony danych dla wykonywania praw osób, których dotyczą dane,

([1]) Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (umowa PNR z 2007 r.) (Dz.U. L 204 z 4.8.2007, str. 18).

([2]) Umowa między Wspólnotą Europejską a Rządem Kanady o przetwarzaniu zaawansowanych informacji o pasażerach oraz zapisu danych dotyczących nazwiska pasażera (Dz.U. L 82 z 21.3.2006, str. 15).

([3]) Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów (Dz.U. L 261 z 6.8.2004, str. 24).

([4]) Najnowsza wersja tego projektu jest dostępna w rejestrze dokumentów Rady pod numerem 16397/07.

([5]) Wspólna opinia w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa, przedstawiona przez Komisję dnia 6 listopada 2007 r., przyjęta przez Grupę Roboczą art. 29 dnia 5 grudnia 2007 r. oraz przez Grupę Roboczą ds. Policji i Wymiaru Sprawiedliwości dnia 18 grudnia 2007 r., WP 145, WPPJ 01/07.

— następnie opinia skupi się na jakości odbiorców danych na szczeblu krajowym. Obawy budzi zwłaszcza charakter biur danych pasażerów, pośredników i właściwych organów wyznaczonych do przeprowadzania analizy zagrożenia i analizy danych pasażerów, gdyż wniosek nie określa go precyzyjnie,

— czwarta kwestia wiąże się z warunkami transferu danych do państw trzecich. Nie jest jasne, jakie warunki będą miały zastosowanie do takiego przekazywania w przypadkach, w których istnieją różne zasady: warunki przekazywania na mocy omawianego wniosku wraz z warunkami określonymi w decyzji ramowej o ochronie danych oraz obowiązujące umowy międzynarodowe (z USA i Kanadą).

11. W ostatniej części zostaną poruszone inne kwestie merytoryczne, w tym kroki poczynione na rzecz ochrony danych, ale też pozostałe budzące zastrzeżenia elementy wniosku.

II. ZGODNOŚĆ PROPONOWANYCH ŚRODKÓW Z PRAWEM

12. Aby przeanalizować zgodność proponowanych środków z prawem w świetle podstawowych zasad ochrony danych, a przede wszystkim art. 8 Karty Praw Podstawowych Unii Europejskiej oraz art. 5–8 konwencji Rady Europy nr 108 ([1]), konieczne jest jednoznaczne określenie celu zamierzonego przetwarzania danych osobowych, co pozwoli na ocenę, czy jest ono niezbędne i proporcjonalne. Należy upewnić się, czy nie istnieją inne, mniej inwazyjne środki, by osiągnąć zamierzony cel.

Określenie celu

13. Sformułowanie wniosku oraz dołączona do niego ocena skutków regulacji wskazują, że celem nie jest po prostu identyfikacja znanych terrorystów lub znanych przestępców uczestniczących w przestępczości zorganizowanej poprzez porównanie ich nazwisk z nazwiskami znajdującymi się w wykazach posiadanych przez organy ochrony porządku publicznego. Celem jest zbieranie informacji wywiadowczych związanych z terroryzmem lub przestępczością zorganizowaną, a dokładniej „ocena zagrożenia związanego z danymi osobami, uzyskiwanie danych wywiadowczych i określanie związków między osobami znanymi i nieznanymi ([2])". Celem określonym w art. 3 ust. 5 wniosku jest, podobnie, „wykrywanie osób, które są *lub mogą być* zaangażowane w przestępstwo terrorystyczne lub przestępczość zorganizowaną, *jak również ich wspólników*".

14. Tę przyczynę podaje się, aby wyjaśnić, że dane API nie wystarczają do osiągnięcia tak określonego celu. Jak wspomniano wcześniej, dane API mają w zamierzeniu pomagać w identyfikacji osób, lecz dane PNR nie mają takiego celu; jednak szczegóły danych PNR przyczyniłyby się do przeprowadzania oceny, czy dana osoba może stanowić zagrożenie, do uzyskiwania informacji wywiadowczych i odnajdywania powiązań między osobami znanymi i nieznanymi.

15. Cel zamierzonych środków obejmuje nie tylko ujęcie osób *znanych*, lecz także określenie osób, które *mogą* spełniać kryteria określone we wniosku.

Głównym elementem wniosku jest więc analiza zagrożeń i określenie wzorców zachowań, co pozwoli zidentyfikować te osoby. Motyw 9 wniosku określa jednoznacznie, że dane muszą być przechowywane „przez odpowiednio długi okres, pozwalający zrealizować cele obejmujące opracowanie wskaźników zagrożenia i ustalenie wzorców w zakresie tras podróży i zachowań".

16. Cel jest zatem podwójny: po pierwsze chodzi o globalny cel zwalczania terroryzmu i przestępczości zorganizowanej, po drugie — o środki i działania nieodłącznie związane z realizacją tego celu. Mimo że cel polegający na zwalczaniu terroryzmu i przestępczości zorganizowanej jest wystarczająco jasny i zgodny z prawem, środki do jego osiągnięcia powinny zostać dalej omówione.

Ustalenie wzorców zachowania i ocena zagrożenia

17. Wniosek nie daje żadnych wskazówek co do sposobu ustalania wzorców zachowania i przeprowadzania oceny zagrożenia. Ocena skutków regulacji precyzuje sposób wykorzystania danych PNR następująco: porównuje się dane PNR „z zestawem cech charakterystycznych oraz wzorców zachowań, w celu opracowania oceny zagrożenia. Jeżeli dany pasażer odpowiada określonej kategorii ryzyka, może on zostać zakwalifikowany do grupy wysokiego ryzyka" ([3]).

18. Podejrzanych można wybierać na podstawie konkretnych elementów ich danych PNR, które wywołują podejrzenia (np. kontakt z podejrzanym biurem podróży, powiadomienie o kradzieży karty kredytowej), oraz na podstawie „wzorców zachowań" lub abstrakcyjnego profilu. Na podstawie wzorców zachowania w podróży rzeczywiście można by określić różne standardowe profile dla „normalnych pasażerów" i „podejrzanych pasażerów". Te profile umożliwiłyby prowadzenie dalszych dochodzeń w stosunku do pasażerów, którzy nie mieszczą się w kategorii „normalnych pasażerów", zwłaszcza, jeżeli wiążą się z innymi podejrzanymi elementami takimi jak kradziona karta kredytowa.

19. Choć nie można przyjmować, że pasażerowie będą oceniani ze względu na swoją religię lub inne wrażliwe dane, wydaje się jednak, że będą przedmiotem dochodzenia na podstawie mieszanki informacji *in concreto* i *in abstracto, włącznie* ze standardowymi wzorcami zachowania i abstrakcyjnymi profilami.

([1]) Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r.

([2]) Uzasadnienie wniosku, rozdział I.

([3]) Ocena skutków regulacji, rozdział 2.1, „Opis problemu".

20. Jest kwestią dyskusyjną, czy taki rodzaj dochodzenia można zakwalifikować jako profilowanie. Profilowanie polega na „stosowaniu metod informatycznych wykorzystujących eksplorację danych z hurtowni danych umożliwiających lub mających umożliwić, z pewnym prawdopodobieństwem — a co za tym idzie, z pewnym marginesem błędu — zaklasyfikowanie danej osoby do konkretnej kategorii, by podjąć w odniesieniu do tej osoby indywidualne decyzje" ([1]).

21. EIOD jest świadomy, że nie zakończyły się dyskusje dotyczące definicji profilowania. Jednak niezależnie od tego, czy oficjalnie przyznano, że wniosek ma na celu *profilowanie* pasażerów, najważniejszym problemem nie są definicje. Chodzi przede wszystkim o konsekwencje dla poszczególnych osób.

22. Główne obawy EIOD wiążą się z faktem, że decyzje dotyczące konkretnych osób będą podejmowane na podstawie wzorców zachowań i kryteriów określonych z wykorzystaniem danych pasażerów w ogóle. W ten sposób decyzje dotyczące jednej osoby mogą zostać podjęte z wykorzystaniem (przynajmniej częściowo) jako punktów odniesienia wzorców opracowanych na podstawie danych *innych* osób. Decyzje będą więc podejmowane w związku z abstrakcyjnym kontekstem, co może mieć znaczące skutki dla osób, których dotyczą dane. Bronienie się osób przed takimi decyzjami jest szczególnie trudne.

23. Ponadto ma się przeprowadzać oceny zagrożenia przy braku jednolitych standardów identyfikacji podejrzanych. EIOD zdecydowanie kwestionuje pewność prawną całego procesu filtrowania, biorąc pod uwagę fakt, że kryteria, według których oceniany będzie każdy pasażer, są źle zdefiniowane.

24. EIOD przywołuje orzecznictwo Europejskiego Trybunału Praw Człowieka, zgodnie z którym prawo krajowe musi być wystarczająco precyzyjne, by wskazać obywatelom, w jakich sytuacjach i na jakich warunkach organy publiczne są uprawnione do gromadzenia i wykorzystywania informacji o życiu prywatnym obywateli. Informacje te „powinny być dostępne dla zainteresowanego, a ich skutki — przewidywalne" ([2]).

25. Podsumowując, omawiany wniosek wymaga dokładnego rozważenia właśnie ze względu na tego rodzaju ryzyko. Choć ogólny cel polegający na walce z terroryzmem i przestępczością zorganizowaną sam w sobie jest jasny i zgodny z prawem, najważniejsze elementy przetwarzania danych, które ma być realizowane, nie wydają się być wystarczająco dobrze określone ani uzasadnione. EIOD wzywa zatem prawodawcę unijnego do zdecydowanego zajęcia się tym problemem przed przyjęciem omawianej decyzji ramowej.

Konieczność

26. Jak wykazano powyżej, ewidentny jest inwazyjny charakter proponowanych środków. Z drugiej strony, nie wykazano jednoznacznie ich przydatności.

27. Ocena skutków wniosku skupia się na najlepszej metodzie ustanowienia systemu PNR w UE, nie zaś na konieczności jego istnienia. W ocenie odniesiono się ([3]) do systemów PNR funkcjonujących w innych krajach, to jest w USA i Zjednoczonym Królestwie. Można jednak ubolewać nad brakiem konkretnych informacji i danych dotyczących tych systemów. Wspomniano „liczne przypadki aresztowań" związanych z „różnymi przestępstwami" w ramach brytyjskiego systemu pilotażowego, nie precyzując ich związków z terroryzmem ani przestępczością zorganizowaną. Brak też szczegółów dotyczących programu USA, z wyjątkiem informacji, że „Unia mogła ocenić wartość danych PNR i docenić ich potencjał do celów egzekwowania prawa".

28. Nie tylko *we wniosku* brak jest dokładnych informacji o konkretnych wynikach stosowania takich systemów PNR, ale i sprawozdania publikowane *przez inne agencje*, np. Government Accountability Office w Stanach Zjednoczonych, nie potwierdzają na obecnym etapie skuteczności tych środków ([4]).

([1]) Definicja ta pochodzi z niedawnego studium profilowania przygotowanego przez Radę Europy: *L'application de la Convention 108 au mécanisme de profilage, Eléments de réflexion destinés au travail futur du Comité consultatif (T-PD)*, Jean-Marc Dinant, Christophe Lazaro, Yves Poullet, Nathalie Lefever, Antoinette Rouvroy, listopad 2007 r. (*dotąd niepublikowane*). Zob. także definicję Lee Bygrave'a: „Ogólnie rzecz biorąc, profilowanie oznacza proces określania zespołu cech (najczęściej dotyczących zachowania) poszczególnych osób lub podmiotów zbiorowych, a następnie traktowanie tej osoby/podmiotu (lub innych osób/podmiotów) w świetle tych cech. Profilowanie jako proces składa się z dwóch głównych elementów: (i) tworzenia profilu — procesu określania profilu; (ii) stosowania profilu — procesu traktowania osób/podmiotów w świetle tego profilu". L. A. BYGRAVE, „Minding the machine: Article 15 of the EC Data Protection Directive and Automated Profiling", *Computer Law & Security Report*, 2001, tom. 17, str. 17–24: http://www.austlii.edu.au/au/journals/PLPR/2000/40.html

([2]) Rotaru przeciwko Rumunii, nr sprawy 28341/95, §§ 50, 52 i 55. Zob. także Amann przeciwko Szwajcarii, nr sprawy 27798/95, §§50 *et s*.

([3]) Rozdział 2.1, „Opis problemu".

([4]) Zob. np. sprawozdanie Government Accountability Office w Stanach Zjednoczonych sporządzone na wniosek członków Kongresu, maj 2007 r. „Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues remain": http://www.gao.gov/new.items/d07346.pdf

29. EIOD uważa, że należy lepiej ocenić techniki polegające na ocenie zagrożenia, jakie stanowią poszczególne osoby, z wykorzystaniem narzędzi eksploracji danych i wzorców zachowania; należy również jasno określić ich użyteczność w ramach walki z terroryzmem, zanim zaczną być stosowane na szeroką skalę.

Proporcjonalność

30. Aby właściwie ocenić bilans ingerencji w prywatność osób i konieczności wprowadzenia środka ([1]), bierze się pod uwagę następujące elementy:

— środki mają zastosowanie do wszystkich pasażerów, niezależnie od tego, czy organy ochrony porządku publicznego prowadzą w ich sprawie dochodzenie, czy nie; środek ten stanowi proaktywne badanie w bezprecedensowej skali,

— decyzje dotyczące konkretnych osób mogą być podejmowane na podstawie abstrakcyjnych profili, są zatem obarczone znaczącym marginesem błędu,

— charakter środków, jakie mają być podjęte przeciwko danej osobie, ma związek z egzekwowaniem prawa: konsekwencje takie jak wyłączenie czy przymus są bardziej inwazyjne niż w innych kontekstach, takich jak oszustwa związane z kartami kredytowymi czy wprowadzaniem towarów do obrotu.

31. Zgodność z zasadą proporcjonalności oznacza nie tylko skuteczność proponowanego środka, ale także to, że cel przewidziany we wniosku nie może zostać osiągnięty z użyciem narzędzi powodujących mniejszą ingerencję w prywatność. Skuteczność proponowanego środka nie została dowiedziona. Należy dokładnie rozważyć istnienie alternatywnych rozwiązań przed wprowadzeniem dodatkowych/nowych środków przetwarzania informacji o osobach. Zdaniem EIOD takiej wszechstronnej oceny nie przeprowadzono.

32. EIOD pragnie przypomnieć inne wielkoskalowe systemy służące monitorowaniu przemieszczania się osób w obrębie granic UE lub osób przekraczających te granice, już funkcjonujące lub mające zostać wdrożone, zwłaszcza wizowy system informacyjny ([2]) i system informacyjny Schengen ([3]). Choć głównym celem tych narzędzi nie jest walka z terroryzmem ani przestępczością zorganizowaną, są one lub będą w jakimś wymiarze dostępne dla organów ochrony porządku publicznego w szerszym zakresie walki z przestępczością ([4]).

33. Inny przykład dotyczy dostępności danych osobowych znajdujących się w krajowych bazach danych policji — zwłaszcza w odniesieniu do danych biometrycznych — w ramach konwencji z Prüm podpisanej w maju 2005 r., której zakres jest rozszerzany na wszystkie państwa członkowskie Unii Europejskiej ([5]).

34. Wszystkie te różne instrumenty umożliwiają globalne monitorowanie przemieszczania się osób, choć z różnych perspektyw. Przed podjęciem decyzji o ustanowieniu nowej formy systematycznego skanowania wszystkich osób wjeżdżających do UE lub wyjeżdżających z niej na pokładzie samolotu, należy przeprowadzić dogłębną i wszechstronną analizę sposobów, w jakie wspomniane wcześniej instrumenty mogą się przyczynić do walki z konkretnymi formami przestępczości, w tym z terroryzmem. EIOD zaleca Komisji przeprowadzenie takiej analizy jako niezbędnego kroku w ramach procedury prawodawczej.

Wniosek

35. W świetle powyższego EIOD stwierdza w odniesieniu do zgodności proponowanych środków z prawem co następuje: opieranie się na różnych bazach danych bez globalnej perspektywy konkretnych wyników i niedociągnięć:

— sprzeciwia się racjonalnej polityce prawodawczej, zgodnie z którą nie należy przyjmować nowych instrumentów, zanim instrumenty istniejące nie zostały w pełni wdrożone i nie dowiedziono ich nieskuteczności ([6]),

— mogłoby poprowadzić w kierunku całkowitego nadzoru nad społeczeństwem.

36. Walka z terroryzmem z całą pewnością może stanowić uzasadnienie dla zastosowania wyjątków od podstawowych praw do prywatności i ochrony danych. By jednak uzasadnienie to było ważne, konieczność ingerencji musi

([1]) Zgodnie z art. 9 konwencji nr 108 „Odstąpienie od stosowania art. 5, 6 i 8 niniejszej Konwencji jest dozwolone, jeśli przewidywane jest ustawowo przez Stronę, jako środek konieczny w społeczeństwie demokratycznym w interesie:
1) ochrony państwa, bezpieczeństwa publicznego, interesów wa1utowych państwa lub zwalczania przestępczości;
2) ochrony podmiotu danych oraz praw i wolności innych osób".

([2]) Decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia wizowego systemu informacyjnego (VIS) (Dz.U. L 213 z 15.6.2004, str. 5); wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, KOM(2004) 0835 wersja ostateczna; wniosek dotyczący decyzji Rady w sprawie wglądu do danych Systemu Informacji Wizowej (VIS) dla organów państw członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw, KOM(2005) 0600 wersja ostateczna.

([3]) Zob. zwłaszcza decyzję Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 205 z 7.8.2007).

([4]) Na ten temat zob.: Opinia Europejskiego Inspektora Ochrony Danych na temat wniosku dotyczącego decyzji Rady w sprawie wglądu do danych systemu informacji wizowej (VIS) dla organów państw członkowskich odpowiedzialnych za bezpieczeństwo wewnętrzne oraz dla Europolu w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom oraz w celu wykrywania i ścigania tych przestępstw (KOM(2005) 600 wersja ostateczna) (Dz.U. C 97 z 25.4.2006, str. 6).

([5]) Zob. opinie EIOD w sprawie decyzji z Prüm: Opinia z dnia 4 kwietnia 2007 r. na temat inicjatywy 15 państw członkowskich w celu przyjęcia decyzji Rady w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem i przestępczością transgraniczną (Dz.U. C 169, 21.7.2007, str. 2), oraz opinia z dnia 19 grudnia 2007 r. na temat inicjatywy Republiki Federalnej Niemiec w sprawie przyjęcia decyzji Rady dotyczącej wdrożenia decyzji 2007/…/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, dostępne na stronie: http://www.edps.europa.eu

([6]) Ta uwaga została zgłoszona przez EIOD kilkakrotnie, ostatnio w opinii z dnia 25 lipca 2007 r. w sprawie wdrażania dyrektywy o ochronie danych (Dz.U. C 255 z 27.10.2007, str. 1).

być poparta jasnymi i niezaprzeczalnymi dowodami; należy też dowieść proporcjonalności przetwarzania danych. Jest to tym bardziej konieczne w przypadku tak szerokiej ingerencji w prywatność poszczególnych osób, jaką przewidziano we wniosku.

37. Można jedynie zauważyć, że we wniosku brak jest takich elementów uzasadnienia oraz że nie przeszedł on testu konieczności i proporcjonalności.

38. EIOD podkreśla, że testy konieczności i proporcjonalności są kwestią podstawową. Stanowią one *condicio sine qua non* wejścia omawianego wniosku w życie. Wszelkie dalsze uwagi EIOD wyrażone w niniejszej opinii należy interpretować w świetle tego wstępnego warunku.

III. OBOWIĄZUJĄCE PRAWO — WYKONYWANIE PRAW OSÓB, KTÓRYCH DOTYCZĄ DANE

Obowiązujące prawo

39. Poniższa analiza skupia się na trzech punktach:

— opisie różnych etapów przetwarzania danych przewidzianego we wniosku, by określić prawo mające zastosowanie do każdego etapu,

— ograniczeniach wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych w odniesieniu do zakresu zastosowania oraz do praw osoby, której dotyczą dane,

— ogólniejszej analizie zakresu, w jakim instrumenty należące do trzeciego filaru mogą mieć zastosowanie do przetwarzania danych w ramach pierwszego filaru przez podmioty prywatne.

Prawo mające zastosowanie do każdego etapu przetwarzania

40. Artykuł 11 omawianego wniosku stanowi, że „państwa członkowskie zapewniają, że decyzja ramowa Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (…) ma zastosowanie do danych przetwarzanych zgodnie z niniejszą decyzją ramową".

41. Mimo tego przepisu nie jest jednak jasne, w jakim zakresie decyzja ramowa o ochronie danych — instrument należący do trzeciego filaru Traktatu UE — będzie miała zastosowanie do danych przetwarzanych przez linie lotnicze, gromadzonych przez biura danych pasażerów, a następnie wykorzystywanych przez inne właściwe organy.

42. Pierwszym etapem przetwarzania danych osobowych przewidzianego we wniosku jest ich przetwarzanie przez linie lotnicze, które są zobowiązane do udostępniania danych PNR — zasadniczo z wykorzystaniem „systemu pchającego" — krajowym biurom danych pasażerów. Ze sformułowania wniosku i oceny jego skutków ([1]) wynika, że dane mogą również być przekazywane partiami przez linie lotnicze pośrednikom. Linie lotnicze prowadzą działalność przede wszystkim w otoczeniu komercyjnym, podlegającym krajowemu prawu w zakresie ochrony danych wdrażającemu dyrektywę 95/46/WE ([2]). Kwestia prawa mającego zastosowanie powstanie, gdy zgromadzone dane będą wykorzystywane do celów ochrony porządku publicznego ([3]).

43. Dane zostaną wtedy przefiltrowane przez pośrednika (w celu ich sformatowania oraz wyłączenia danych PNR nie znajdujących się w wykazie danych wymaganych na mocy wniosku) lub przesłane bezpośrednio biurom danych pasażerów. Pośrednicy mogą być podmiotami sektora prywatnego, jak na przykład firma SITA, działająca jako pośrednik w ramach umowy o PNR z Kanadą.

44. Jeżeli chodzi o biura danych pasażerów, odpowiedzialne za ocenę ryzyka związaną ze wszystkimi danymi, nie jest jasne, kto będzie ponosił odpowiedzialność za przetwarzanie tych danych. W przetwarzanie mogą być zaangażowane organy celne i dokonujące kontroli granicznej, niekoniecznie organy ochrony porządku publicznego.

45. Następujące później przekazanie przefiltrowanych danych „właściwym" organom prawdopodobnie będzie się odbywać w kontekście egzekwowania prawa. Zgodnie z wnioskiem „właściwe organy obejmują wyłącznie organy odpowiedzialne za zapobieganie przestępstwom terrorystycznym i przestępczości zorganizowanej oraz ich zwalczanie".

46. Podmioty zaangażowane w kolejne etapy przetwarzania danych oraz realizowany cel coraz ściślej wiążą się ze współpracą policyjną i sądową w sprawach karnych. We wniosku nie określono jednak jednoznacznie, kiedy ma zastosowanie decyzja ramowa o ochronie danych. Brzmienie wniosku mogłoby nawet prowadzić do uznania, że ma ona zastosowanie do całego procesu przetwarzania, a nawet do linii lotniczych ([4]). Decyzja ramowa o ochronie danych sama w sobie zawiera jednak pewne ograniczenia.

([1]) Artykuł 6 ust. 3 wniosku oraz ocena skutków, załącznik A, „Metody przekazywania danych przez przewoźników".

([2]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, str. 31).

([3]) Pod tym względem zob. konsekwencje wyroku w sprawie danych PNR. Wyrok Trybunału z 30 maja 2006 r., Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji (C-318/04), sprawy połączone C-317/04 i C-318/04, Zb. Orz. 2006, pkt 56.

([4]) Artykuł 11 wniosku. Zob. także motyw 10 preambuły: „Decyzja ramowa Rady (…) w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych powinna mieć zastosowanie do wszystkich danych przetwarzanych zgodnie z niniejszą decyzją ramową. Prawa osób, których dotyczą dane, związane z takim przetwarzaniem, takie jak prawo do uzyskania informacji, prawo dostępu do danych, prawo do sprostowania, usunięcia lub zablokowania danych oraz prawo do odszkodowania i do środków ochrony sądowej powinny zostać przewidziane na podstawie niniejszej decyzji ramowej".

47. W tym kontekście EIOD ma wątpliwości przede wszystkim co do tego, czy tytuł VI Traktatu UE może rutynowo służyć jako podstawa prawna dla zobowiązań prawnych w stosunku do podmiotów sektora prywatnego. Ponadto istotne jest również pytanie, czy tytuł VI Traktatu UE może służyć jako podstawa prawna dla zobowiązań prawnych organów publicznych, które zasadniczo znajdują się poza ramami współpracy na rzecz ochrony porządku publicznego. Pytania te zostaną pełniej opracowane w dalszej części niniejszej opinii.

Ograniczenia decyzji ramowej o ochronie danych

48. Tekst wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych zawiera co najmniej dwa ograniczenia zakresu zastosowania.

49. Po pierwsze, zakres zastosowania decyzji ramowej o ochronie danych jest dokładnie określony w samej tej decyzji: ma ona zastosowanie „wyłącznie do danych gromadzonych lub przetwarzanych przez właściwe organy w celu zapobiegania przestępstwom, ich ścigania, wykrywania lub karania albo w celu wykonywania sankcji karnych" ([1]).

50. Po drugie, decyzja ramowa o ochronie danych nie ma mieć zastosowania do danych przetwarzanych wyłącznie na szczeblu krajowym, lecz jej stosowanie jest ograniczone do danych wymienianych między państwami członkowskimi i przekazywanych dalej do państw trzecich ([2]).

51. W porównaniu do dyrektywy 95/46/WE decyzja ramowa o ochronie danych ma również kilka wad, w szczególności znaczne odstępstwo od zasady ograniczenia celu. W odniesieniu do tej zasady, wniosek wyraźnie ogranicza cel przetwarzania danych do walki z terroryzmem i przestępczością zorganizowaną. Decyzja ramowa o ochronie danych zezwala jednak na przetwarzanie danych w szerzej określonych celach. W takim przypadku *lex specialis* (wniosek) należy przyznać większą wagę niż *lex generalis* (decyzja ramowa o ochronie danych) ([3]). Należy to jednoznacznie określić w tekście wniosku.

52. Z tego powodu EIOD zaleca dodanie do wniosku następującego przepisu: „Dane osobowe przekazywane przez linie lotnicze zgodnie z niniejszą decyzja ramową nie mogą być przetwarzane do celów innych niż walka z terroryzmem i przestępczością zorganizowaną. Wyjątki w odniesieniu do zasady ograniczenia celu przewidziane w decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych nie mają zastosowania".

53. Podsumowując, EIOD zauważa poważny brak pewności prawnej w odniesieniu do systemu ochrony danych mającego zastosowanie do różnych podmiotów uczestniczących w przedsięwzięciu, a szczególnie linii lotniczych i innych podmiotów należących do pierwszego filaru: niezależnie od tego, czy chodzi o przepisy wniosku, przepisy decyzji ramowej o ochronie danych czy ustawodawstwo krajowe wdrażające dyrektywę 95/46/WE. Prawodawca powinien wyjaśnić, w którym dokładnie momencie przetwarzania danych będą miały zastosowanie te różne przepisy.

Warunki stosowania zasad odnoszących się do pierwszego i trzeciego filaru

54. EIOD kwestionuje z zasady fakt, że instrument należący do trzeciego filaru tworzy rutynowo w celach ochrony porządku publicznego zobowiązania prawne w stosunku do podmiotów sektora prywatnego lub publicznego, które w zasadzie znajdują się poza ramami współpracy na rzecz ochrony porządku publicznego.

55. Można by przeprowadzić porównanie z dwoma innymi przypadkami, w których sektor prywatny był zaangażowany w zatrzymywanie lub przekazywanie danych w kontekście ochrony porządku publicznego:

— *przypadek umowy o PNR z USA, który przewidywał systematyczne przekazywanie przez linie lotnicze danych PNR organom ochrony porządku publicznego*. Wyrok Trybunału Sprawiedliwości w sprawie PNR wykluczył kompetencje Wspólnoty do zawarcia umowy w sprawie PNR. Jedno z uzasadnień stanowił fakt, że przekazywanie danych PNR do amerykańskiego CBP (Customs and Border Protection) stanowi operację przetwarzania danych dotyczącą bezpieczeństwa publicznego i działalności państwa w dziedzinie prawa karnego ([4]). W tym przypadku operacja przetwarzania danych oznaczała ich przekazywanie do CBP *w sposób systematyczny*, co odróżnia go od poniższego przypadku:

— *ogólne zatrzymywanie danych przez operatorów łączności elektronicznej*. W odniesieniu do kompetencji Wspólnoty, by ustanowić taki okres przechowywania, można zauważyć różnicę z przypadkiem umowy o PNR z USA, zważając na to, że dyrektywa 2006/24/WE ([5]) przewiduje wyłącznie zobowiązanie do zatrzymywania danych, które pozostają pod kontrolą operatorów. Nie przewidziano systematycznego przekazywania danych organom ochrony porządku publicznego. Można więc stwierdzić, że — póki dane pozostają pod kontrolą dostawców usług — dostawcy usług ponoszą odpowiedzialność za poszanowanie obowiązku ochrony danych osobowych w stosunku do osoby, której te dane dotyczą.

([1]) Motyw 5a, wersja decyzji ramowej o ochronie danych z dnia 11 grudnia 2007 r.
([2]) Artykuł 1.
([3]) Odnośnie do tego punktu należy dokładnie rozważyć i omówić brzmienie art. 27b najnowszego projektu decyzji ramowej o ochronie danych w trzecim filarze.
([4]) Wyrok Trybunału z 30 maja 2006 r., Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji (C-318/04), sprawy połączone C-317/04 i C-318/04, Zb. Orz. 2006, pkt 56.
([5]) Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, (Dz.U. L 105 z 13.4.2006, str. 54).

56. Zgodnie z omawianym wnioskiem dotyczącym PNR w UE linie lotnicze muszą systematycznie udostępniać dane PNR wszystkich pasażerów. Dane te nie są jednak przekazywane partiami bezpośrednio organom ochrony porządku publicznego: mogą zostać przesłane pośrednikowi i są oceniane przez stronę trzecią o niejasnym statusie, zanim wybrane informacje zostają przesłane właściwym organom.

57. Większa część procesu przetwarzania danych ma miejsce w „szarej strefie" powiązanej zasadniczo zarówno z pierwszym, jak i z trzecim filarem. Charakter podmiotów przetwarzających te dane nie jest jasny, co zostanie omówione w rozdziale IV. Linie lotnicze ewidentnie nie są organami ochrony porządku publicznego, a pośrednicy mogą być podmiotami sektora prywatnego. Nawet w odniesieniu do biur danych pasażerów, które będą organami publicznymi, należy podkreślić, że nie każdy organ publiczny spełnia wymagania i posiada kompetencje, aby rutynowo pełnić zadania związane z ochroną porządku publicznego.

58. Tradycyjnie istniał jasny podział między działaniami organów ochrony porządku publicznego a działaniami sektora prywatnego, gdyż zadania związane z ochroną porządku publicznego są pełnione przez specjalnie wyznaczone organy, a od podmiotów prywatnych wymaga się w konkretnym przypadku przekazania tym organom danych osobowych. Obecnie istnieje tendencja do systematycznego nakładania na podmioty prywatne obowiązku współpracy z organami ochrony porządku publicznego, co wiąże się z pytaniem, które ramy ochrony danych (należące do pierwszego czy trzeciego filaru) mają zastosowanie do warunków tej współpracy: czy przepisy powinny być oparte na cechach administratora danych (sektor prywatny) czy na celu, który ma zostać osiągnięty (ochrona porządku publicznego)?

59. EIOD przypomniał już ryzyko luki prawnej między działaniami w ramach pierwszego i trzeciego filaru ([1]). Rzeczywiście nie jest jasne, które działania firm prywatnych, w pewien sposób związane z egzekwowaniem prawa karnego, są objęte zakresem działania prawodawcy Unii Europejskiej na mocy art. 30, 31 i 34 Traktatu UE.

60. Jeżeli nie mają zastosowania ramy ogólne (pierwszy filar), dostawca usług byłby zobowiązany do wprowadzenia trudnych rozróżnień w obrębie swoich baz danych. W obowiązującym systemie jasne jest, że administrator danych musi stosować w odniesieniu do osób, których dane dotyczą, te same zasady ochrony danych niezależnie od celów, jakie uzasadniają zatrzymywanie tych danych. Należy zatem unikać sytuacji, której rezultatem byłoby objęcie przetwarzania danych przez dostawców usług różnymi ramami ochrony danych w zależności od celu przetwarzania.

Wykonywanie praw przysługujących osobom, których dotyczą dane

61. Różne systemy prawne, które miałyby zastosowanie na szczeblu krajowym, miałyby przede wszystkim znaczący wpływ na korzystanie przez osoby, których dotyczą dane, z przysługujących im praw.

62. W preambule wniosku określono, że „prawo do uzyskania informacji, prawo dostępu do danych, prawo do sprostowania, usunięcia lub zablokowania danych oraz prawo do odszkodowania i do środków ochrony sądowej powinny zostać przewidziane na podstawie niniejszej decyzji ramowej". Stwierdzenie to nie stanowi jednak odpowiedzi na pytanie, kim jest administrator danych odpowiedzialny za reagowanie na wnioski osób, których dotyczą dane.

63. Choć linie lotnicze mogłyby podawać informacje o przetwarzaniu danych, sytuacja komplikuje się, gdy w grę wchodzi dostęp do danych lub ich prostowanie. Decyzja ramowa o ochronie danych faktycznie ogranicza uprawnienia do wykonywania tych działań. Jak stwierdzono wcześniej, jest wątpliwe, czy dostawca usług taki jak linia lotnicza mógłby zostać zobligowany do stworzenia różnych ścieżek dostępu do danych, które posiada, i uprawnień do prostowania tych danych w zależności od celu tych czynności (handlowego lub związanego z ochroną porządku publicznego). Można by dowodzić, że prawa te powinny być wykonywane przed przekazaniem danych do biur danych pasażerów lub innych wyznaczonych właściwych organów. Wniosek nie zawiera jednak żadnych dalszych wskazówek w tym zakresie i — jak wspomniano wcześniej — nie jest jasne, czy te organy (przynajmniej biura danych pasażerów) będą organami ochrony porządku publicznego normalnie korzystającymi z procedur ograniczonego (w miarę możliwości niebezpośredniego) dostępu.

64. Osobie, której dotyczą dane, grozi również ryzyko przekazania jej danych różnym odbiorcom, jeżeli chodzi o biura danych pasażerów: dane są w rzeczywistości przekazywane do biura w kraju wylotu/przylotu, ale w poszczególnych przypadkach mogą być również przekazywane biurom danych pasażerów w innych państwach członkowskich. Ponadto jest możliwe utworzenie lub wyznaczenie przez kilka państw członkowskich jednego wspólnego biura. W takim przypadku osoba, której dotyczą dane, mogłaby być zmuszona do podejmowania środków odwoławczych przed organem innego państwa członkowskiego. Należy jednak ponownie zauważyć, że nie jest jasne, czy zastosowanie będą miały krajowe przepisy ochrony danych (jest przewidziana ich harmonizacja w obrębie UE), czy też trzeba będzie uwzględnić szczególne prawodawstwo dotyczące ochrony porządku publicznego (biorąc pod uwagę, że kwestie dotyczące trzeciego filaru na szczeblu krajowym nie zostały wszechstronnie zharmonizowane).

65. To samo pytanie odnosi się do dostępu do danych przetwarzanych przez pośredników, których status nie jest jasny i którzy mogą świadczyć usługi wspólnie dla kilku linii lotniczych z różnych państw członkowskich UE.

([1]) Zob. opinia 2007/C 255/01 Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (Dz.U. C 255 z 27.10.2007, str. 1). Zob. także sprawozdanie roczne za 2006 r., str. 47.

66. EIOD wyraża ubolewanie z powodu ciągłego braku pewności odnośnie do korzystania przez osoby, których dotyczą dane, ze swoich podstawowych praw. Podkreśla, że sytuacja ta wynika przede wszystkim z faktu, że podmioty, których podstawowym zadaniem nie jest ochrona porządku publicznego, obarcza się odpowiedzialnością za nią.

Wniosek

67. EIOD uważa, że wniosek powinien jasno określać, który system prawny ma zastosowanie do każdego etapu przetwarzania danych oraz w odniesieniu do którego podmiotu czy organu można korzystać z prawa do dostępu i do środków odwoławczych. EIOD przypomina, że zgodnie z art. 30 ust. 1 lit. b) Traktatu UE przepisy dotyczące ochrony danych powinny być właściwe i obejmować pełny zakres operacji przetwarzania danych określonych we wniosku. Proste odniesienie do decyzji ramowej o ochronie danych nie wystarcza, biorąc pod uwagę ograniczony zakres zastosowania tej decyzji oraz zawarte w niej ograniczenie uprawnień. W odniesieniu do organów ochrony porządku publicznego przepisy decyzji ramowej o ochronie danych powinny mieć zastosowanie co najmniej do całości przetwarzania danych przewidzianego we wniosku, by zagwarantować spójne stosowanie zasad ochrony danych.

IV. CHARAKTER ODBIORCÓW DANYCH

68. EIOD zauważa, że wniosek nie przewiduje żadnej specyfikacji cech odbiorców danych osobowych gromadzonych przez linie lotnicze, czy to dla pośredników, czy też dla biur danych pasażerów lub właściwych organów. Należy podkreślić, że charakter odbiorcy danych jest bezpośrednio związany z rodzajem gwarancji dotyczących ochrony danych, które mają zastosowanie do tego odbiorcy. Wcześniej wspomniano już różnicę między gwarancjami oferowanymi w ramach zasad dotyczących pierwszego i trzeciego filaru. Kwestią zasadniczą jest, by mający zastosowanie system był jasny dla wszystkich zainteresowanych podmiotów, w tym rządów poszczególnych państw, agencji ochrony porządku publicznego, organów ochrony danych oraz administratorów danych i osób, których te dane dotyczą.

Pośrednicy

69. Wniosek nie zawiera żadnych wskazówek co do charakteru pośredników ([1]). Nie określono także roli pośredników jako administratorów danych lub podmiotów je przetwarzających. Na podstawie dotychczasowego doświadczenia wydaje się, że podmiotom sektora prywatnego, np. komputerowemu systemowi rezerwacji lub innej jednostce, bez problemów można by powierzyć zadanie gromadzenia danych PNR bezpośrednio od linii lotniczych, by następnie przekierować je do biur danych pasażerów. Dane faktycznie są przetwarzane w taki sposób na mocy umowy o PNR z Kanadą. Za przetwarzanie informacji odpowiedzialne jest przedsiębiorstwo SITA ([2]). Rola pośrednika jest zasadnicza, gdyż może on być odpowiedzialny za wychwytywanie/przeformatowywanie danych przekazywanych przez linie lotnicze całymi partiami ([3]). Nawet jeżeli pośrednicy są zobowiązani do usunięcia przetwarzanych informacji po ich przekazaniu biurom danych pasażerów, sam proces przetwarzania jest wysoce problematyczny: konsekwencją udziału pośredników jest utworzenie dodatkowej bazy danych obejmującej ogromne ilości danych, a nawet — zgodnie z wnioskiem — danych wrażliwych (od pośredników wymaga się następnie usunięcia tych danych). W związku z powyższym EIOD zaleca, by w proces przetwarzania danych pasażerów nie włączać pośredników, o ile ich charakter i zadania nie zostaną precyzyjnie określone.

Biura danych pasażerów

70. Biura danych pasażerów odgrywają zasadniczą rolę w identyfikacji osób, które są lub mogą być zaangażowane w działania terrorystyczne lub przestępczość zorganizowaną lub związane z działaniami terrorystycznymi lub przestępczością zorganizowaną. Zgodnie z wnioskiem biura te będą odpowiedzialne za ustalanie wskaźników ryzyka i udzielanie informacji wywiadowczych dotyczących wzorców w zakresie tras podróży ([4]). Gdy ocena zagrożenia jest oparta na standardowych wzorcach w zakresie tras podróży, a nie na materialnych dowodach odpowiadających konkretnej sprawie, analizę można uznać za proaktywną technikę śledczą. EIOD podkreśla, że ten rodzaj przetwarzania danych zasadniczo jest dokładnie uregulowany prawem poszczególnych państw członkowskich (o ile nie jest zabroniony) i że powierzono go konkretnym organom publicznym, których funkcjonowanie jest również ściśle uregulowane.

71. Biurom danych pasażerów powierza się zatem bardzo wrażliwy rodzaj przetwarzania informacji, przy czym wniosek nie zawiera żadnych szczegółów dotyczących charakteru tych biur ani warunków, na jakich miałyby korzystać z tych kompetencji. Choć jest prawdopodobne, że zadanie to będzie wykonywane przez organ rządowy, być może organy celne lub organy kontroli granicznej, wniosek nie uniemożliwia wyraźnie państwom członkowskim powierzenia go agencjom wywiadowczym lub jakiemukolwiek innemu podmiotowi. EIOD podkreśla, że przejrzystość i gwarancje mające zastosowanie do agencji wywiadowczych nie zawsze są tożsame z tymi, które mają zastosowanie do tradycyjnych organów ochrony porządku publicznego. Szczegółowe informacje o charakterze biur danych pasażerów mają zasadniczą wagę, gdyż niosą ze sobą bezpośrednie skutki dla mających zastosowanie ram prawnych oraz warunków nadzoru. EIOD uważa, że wniosek musi zawierać dodatkowy przepis szczegółowo opisujące specyficzne cechy tych biur.

([1]) Artykuł 6 wniosku.

([2]) SITA została utworzona w 1949 roku przez 11 linii lotniczych. Firma komercyjna SITA INC (Information, Networking Computing — Informacje, Sieci, Usługi Informatyczne) zapewnia branży przewozów lotniczych rozwiązania wnoszące wartość dodaną, a SITA SC świadczy usługi sieciowe; obydwie firmy działają na zasadzie spółdzielczej.

([3]) Ocena skutków, załącznik A, „Metody przekazywania danych przez przewoźników".

([4]) Artykuł 3 wniosku.

Właściwe organy

72. Z art. 4 wniosku wynika, że jakikolwiek organ odpowiedzialny za zapobieganie przestępstwom terrorystycznym i przestępczości zorganizowanej oraz walkę z nimi może otrzymywać dane. Choć jasno określony został cel, brak informacji o charakterze tego organu. We wniosku nie przewidziano żadnego ograniczenia podmiotów otrzymujących dane do organów ochrony porządku publicznego.

Jak wspomniano powyżej w odniesieniu do biur danych pasażerów, zasadniczą kwestią jest, by wrażliwe informacje, o których mowa, były przetwarzane w otoczeniu ujętym w jasne ramy prawne. Jest to tym istotniejsze w przypadku np. organów ochrony porządku publicznego, a nie agencji wywiadowczych. Biorąc pod uwagę elementy eksploracji danych i proaktywnych technik śledczych zawarte we wniosku, nie można wykluczyć zaangażowania takich agencji wywiadowczych w przetwarzanie danych, nie wyłączając innego rodzaju organów.

Wniosek

73. W ramach komentarza natury ogólnej EIOD zauważa, że wdrożenie systemu PNR w UE staje się coraz trudniejsze, biorąc pod uwagę fakt, że organy ochrony porządku publicznego mają różne kompetencje w zależności od prawa krajowego państw członkowskich, obejmujące lub nie operacje wywiadowcze, kontrolę podatkową, imigracyjną lub działania policyjne. Stanowi to jednak dodatkowy powód, by zalecić znaczne sprecyzowanie wniosku w odniesieniu do charakteru wspomnianych podmiotów oraz gwarancji dotyczących nadzoru nad wykonywaniem ich zadań. Do wniosku należy dodać przepisy ściśle określające kompetencje i zobowiązania prawne przewoźników, biur danych pasażerów i innych właściwych organów.

V. **WARUNKI TRANSFERU DANYCH DO PAŃSTW TRZECICH**

74. Wniosek przewiduje pewne zabezpieczenia związane z transferem danych PNR do państw trzecich ([1]). W szczególności jednoznacznie określa zastosowanie decyzji ramowej o ochronie danych do przekazywania danych, zawiera konkretne ograniczenie celu i stwierdza potrzebę wyrażenia przez dane państwo członkowskie zgody w przypadku przekazania danych dalej. Przekazanie danych powinno również być zgodne z prawem krajowym zainteresowanego państwa członkowskiego oraz z wszelkimi mającymi zastosowanie umowami międzynarodowymi.

75. Pozostaje jednak wiele pytań, zwłaszcza w odniesieniu do charakteru tej zgody, warunków stosowania decyzji ramowej o ochronie danych oraz wzajemności w przekazywaniu danych do państw trzecich.

([1]) Artykuł 8 wniosku.

Charakter zgody

76. Państwo członkowskie, z którego pochodzą dane, musi wydać wyraźną zgodę na dalszy transfer danych z jednego państwa trzeciego do innego. We wniosku nie określono, na jakich warunkach i przez kogo wydawana jest ta zgoda i czy krajowe organy ochrony danych powinny być zaangażowane w ten proces. EIOD uważa, że sposób, w jaki będzie wydawana zgoda, powinien być co najmniej zgodny z prawem krajowym poszczególnych państw określającym warunki transferu danych osobowych do państw trzecich.

77. Ponadto zgoda państwa członkowskiego nie powinna mieć większego znaczenia niż zasada, zgodnie z którą państwo otrzymujące dane musi przewidzieć właściwy poziom ochrony zamierzanej operacji przetwarzania. Warunki te powinny się kumulować, podobnie jak w decyzji ramowej o ochronie danych (art. 14). EIOD proponuje zatem, by do art. 8 ust. 1 dodać lit. c) w brzmieniu: „oraz c) kraj trzeci zapewnia właściwy poziom ochrony zamierzanej operacji przetwarzania". EIOD przypomina w tym kontekście, że należy wprowadzić mechanizmy gwarantujące wspólne standardy i koordynację decyzji w odniesieniu do tego, co uważane jest za właściwe ([2]).

Stosowanie decyzji ramowej o ochronie danych

78. Wniosek odnosi się do warunków i zabezpieczeń zawartych w decyzji ramowej o ochronie danych, określając również wyraźnie pewne warunki, zwłaszcza omówioną powyżej zgodę zainteresowanego państwa członkowskiego oraz ograniczenie celu do zapobiegania przestępstwom terrorystycznym i przestępczości zorganizowanej oraz walki z nimi.

79. Sama decyzja ramowa o ochronie danych określa warunki transferu danych osobowych do państw trzecich, w tym co się tyczy ograniczenia celu, charakteru podmiotów otrzymujących dane, zgody państwa członkowskiego i zasady odpowiedniej ochrony. Przewiduje jednak również odstępstwa od tych warunków: uzasadniony interes ogólny, zwłaszcza ważny interes publiczny, może być wystarczającą podstawą przekazania danych, nawet jeżeli nie spełniono wymienionych powyżej warunków.

80. Jak wspomniano już w rozdziale III niniejszej opinii, EIOD uważa, że należy jasno określić w tekście wniosku, iż bardziej szczegółowe gwarancje zawarte we wniosku mają pierwszeństwo przed ogólnymi warunkami — i wyjątkami — ustalonymi w decyzji ramowej o ochronie danych, tam gdzie ma ona zastosowanie.

([2]) Opinia EIOD z dnia 26 czerwca 2007 r. w sprawie wniosku dotyczącego decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, pkt 27–30 (Dz.U. C 139 z 23.6.2007, str. 1).

Zasada wzajemności

81. W wniosku zajęto się kwestią ewentualnych „wniosków odwetowych" składanych przez państwa, które mogą się zwracać do UE o dane PNR dotyczące lotów z UE na ich terytorium. Jeżeli UE zwraca się o dane pochodzące z baz danych linii lotniczych państw trzecich, gdyż prowadzą one loty do lub z UE, dane państwo trzecie powinno zwrócić się o to samo do linii lotniczych mających siedzibę w UE, w tym, o dane obywateli UE. Choć Komisja uważa, że prawdopodobieństwo takich żądań jest „bardzo niewielkie", dopuszcza je. Wniosek odnosi się w tym względzie do faktu, że umowy z USA i z Kanadą przewidują takie wzajemne przekazywanie danych, „które może zostać wprowadzone w życie automatycznie" ([1]). EIOD ma wątpliwości co do znaczenia takiej automatycznej wzajemności oraz stosowania zabezpieczeń do tego rodzaju przekazywania danych, przede wszystkim uwzględniając istnienie w danym państwie właściwego poziomu ochrony.

82. Należy wprowadzić rozróżnienie między państwami trzecimi, które już zawarły umowę z UE, i tymi, które takiej umowy nie zawarły.

Państwa, które nie zawarły umowy z UE

83. EIOD zauważa, że wzajemność mogłaby prowadzić do przekazywania danych osobowych państwom, które nie gwarantują standardów demokratycznych ani właściwego poziomu ochrony danych.

84. Ocena skutków regulacji zawiera dalsze elementy związane z warunkami przekazywania danych do państw trzecich: podkreślono korzyści płynące ze stosowania systemu PNR w UE, gdyż dane są w nim filtrowane przez biura danych pasażerów. Tylko wybrane dane osób podejrzanych (a nie wszystkie zgromadzone dane) byłyby przekazywane właściwym organom państw członkowskich i prawdopodobnie także państwom trzecim ([2]). EIOD zaleca wyjaśnienie tego punktu w tekście wniosku. Zwykłe stwierdzenie w ocenie skutków regulacji nie zapewnia koniecznej ochrony.

85. Choć selekcja danych przyczyniłaby się do zmniejszenia ingerencji w prywatność pasażerów, należy przypomnieć, że zasady ochrony danych wychodzą daleko poza zmniejszanie ilości danych, i obejmują konieczność, przejrzystość i wykonywanie praw osób, których dotyczą dane; wszystkie te zasady należy brać pod uwagę podczas oceny, czy dane państwo trzecie zapewnia właściwy poziom ochrony.

Państwa, które zawarły umowę dwustronną z UE

86. Ocena skutków regulacji wskazuje, że taki rodzaj przetwarzania danych umożliwi UE „kładzenie nacisku na spełnienie pewnych standardów oraz zapewnienie spójności w takich dwustronnych umowach z państwami trzecimi. Umożliwi również żądanie traktowania w taki sam sposób przez państwa trzecie, z którymi UE zawarła umowę, co nie jest obecnie możliwe" ([3]).

87. Z tych uwag wynika pytanie o skutki wniosku dla obowiązujących umów z Kanadą i USA. Warunki dostępu do danych określone w tych umowach są zaiste o wiele szersze, gdyż dane nie są poddawane selekcji przed ich przekazaniem tym państwom trzecim.

88. Ocena skutków regulacji wskazuje, że „w przypadkach, w których UE zawarła z państwem trzecim umowę międzynarodową dotyczącą wymiany/przekazywania danych PNR do takiego państwa trzeciego, należy te umowę uwzględnić. Przewoźnicy powinny przesyłać dane PNR biurom danych pasażerów zgodnie z normalnymi praktykami na mocy obowiązujących przepisów. Biuro danych pasażerów otrzymujące takie dane powinno przekazać je właściwemu organowi państwa trzeciego, z którym zawarto umowę" ([4]).

89. Z jednej strony celem wniosku wydaje się być przekazywanie jakiemukolwiek właściwemu organowi, w UE lub poza nią, *wyłącznie wybranych* danych, zaś z drugiej — ocena skutków regulacji, preambuła wniosku (motyw 21) i sam art. 11 przypominają, że należy odpowiednio uwzględnić obowiązujące umowy. Mogłoby to prowadzić do wniosku, że filtrowanie danych może odnosić się wyłącznie do umów, które zostaną zawarte w przyszłości. Z tej perspektywy można przewidzieć, że dostęp do całej partii danych będzie nadal obowiązywał np. w przypadku dostępu organów USA do danych PNR, zgodnie z przepisami umowy UE–USA, ale że równolegle i w poszczególnych przypadkach mogą być przekazywane do USA również konkretne dane wyselekcjonowane przez biura danych pasażerów, obejmujące dane dotyczące lotów do USA, ale nie ograniczone do nich.

90. EIOD wyraża ubolewanie z powodu braku jasności w tym zasadniczym punkcie wniosku. Uważa za kwestię kluczową spójność warunków transferu danych PNR do państw trzecich oraz podleganie tych warunków ujednoliconemu poziomowi ochrony. Ponadto, ze względu na pewność prawną, należy w samym wniosku — a nie tylko w ocenie skutków regulacji jak obecnie — sprecyzować zabezpieczenia mające zastosowanie do przekazywania danych.

([1]) Uzasadnienie wniosku, rozdział 2.
([2]) Ocena skutków, rozdział 5 pkt 2, „Ochrona prywatności".
([3]) Ocena skutków, rozdział 5 pkt 2, „Stosunki z państwami trzecimi".
([4]) Ocena skutków, załącznik A, „Podmioty otrzymujące dane od biur danych pasażerów".

VI. **INNE KWESTIE MERYTORYCZNE**

Automatyczne przetwarzanie

91. EIOD zauważa, że wniosek wyraźnie wyłącza podejmowanie działań związanych z egzekwowaniem prawa przez biura danych pasażerów i właściwe organy państw członkowskich wyłącznie na podstawie automatycznego przetwarzania danych PNR lub z powodu pochodzenia rasowego lub etnicznego, przekonań religijnych lub filozoficznych, poglądów politycznych lub orientacji seksualnej danej osoby ([1]).

92. EIOD przyjmuje to z zadowoleniem, gdyż takie wyłączenie ogranicza ryzyko podejmowania arbitralnych działań w stosunku do pojedynczych osób. Zauważa jednak, że zakres tego wyłączenia ogranicza się do *działań związanych z egzekwowaniem prawa* podejmowanych przez biura danych pasażerów i właściwe organy państw członkowskich. Wyłączenie to w obecnej wersji tekstu nie obejmuje automatycznego filtrowania osób na podstawie standardowych profili ani nie uniemożliwia automatycznego tworzenia list osób podejrzanych i podejmowania takich środków jak rozszerzony nadzór, o ile nie są one uznawane za działania związane z egzekwowaniem prawa.

93. EIOD uważa, że pojęcie *działań związanych z egzekwowaniem prawa* jest zbyt mało precyzyjne i że z reguły nie należy podejmować *żadnych decyzji* odnoszących się do poszczególnych osób *wyłącznie* na podstawie automatycznego przetworzenia ich danych ([2]). EIOD zaleca odpowiednią zmianę wniosku.

Jakość danych

94. W art. 5 ust. 2 wniosku znajduje się istotne wyjaśnienie, że nie nakłada się na linie lotnicze zobowiązania do gromadzenia lub zatrzymywania danych uzupełniających dane gromadzone pierwotnie w celach komercyjnych.

95. Kilka aspektów przetwarzania tych danych zasługuje na dalszą uwagę:

— wykaz danych, które mają być udostępniane, zgodnie z załącznikiem 1 do wniosku, jest bardzo obszerny i przypomina wykaz danych udostępnianych organom USA zgodnie z umową UE–USA. Jakość niektórych rodzajów tych danych była już kilkakrotnie kwestionowana przez organy ochrony danych, a zwłaszcza przez Grupę Roboczą art. 29 ([3]),

— ze sformułowania oceny skutków regulacji ([4]) i art. 6 ust. 3 wniosku wynika, że dane mogą również być przekazywane partiami przez linie lotnicze pośrednikom. Na pierwszym etapie dane przekazywane stronie trzeciej nie byłyby nawet ograniczone zgodnie z wykazem danych PNR zawartym w załączniku 1 do wniosku,

— w odniesieniu do przetwarzania danych wrażliwych, nawet jeżeli mogłyby one zostać odfiltrowane przez pośredników, pozostaje pytanie, czy przekazywanie przez linie lotnicze pól otwartych jest naprawdę konieczne.

EIOD popiera dotyczące tych kwestii punkty opinii Grupy Roboczej art. 29.

Metody przekazywania danych PNR

96. Od przewoźników lotniczych mających siedzibę poza UE wymaga się dostarczania danych (metoda „*push*") do biur danych pasażerów, o ile posiadają umożliwiającą to infrastrukturę. Jeżeli dostarczenie danych nie jest możliwe, muszą umożliwić pobieranie danych (metoda „*pull*").

97. Zezwolenie na różne metody przekazywania danych z zależności od linii lotniczej zwiększy jedynie trudności co do kontroli przestrzegania zasad ochrony danych podczas przekazywania danych PNR. Grozi to również zakłóceniem konkurencji pomiędzy liniami lotniczymi z UE i spoza niej.

98. EIOD przypomina, że metoda dostarczania, umożliwiająca liniom lotniczym utrzymanie kontroli nad jakością przekazywanych danych oraz warunkami ich przekazywania, jest jedyną metodą dopuszczalną ze względu na proporcjonalność procesu przetwarzania danych. Ponadto musi ona polegać na rzeczywistym dostarczaniu, tzn. dane nie powinny być wysyłane partiami do pośrednika, lecz filtrowane na samym początku procesu. Jest niedopuszczalne, by dane nie uznane za niezbędne — oraz dane nieujęte w załączniku 1 do wniosku — były przesyłane stronie trzeciej, nawet jeżeli ta strona trzecia miałaby je natychmiast usunąć.

Zatrzymywanie danych

99. Artykuł 9 wniosku przewiduje 5-letni okres przechowywania danych PNR oraz dodatkowy okres 8 lat, podczas których dane są przechowywane w archiwalnej bazie danych dostępnej pod ściśle określonymi warunkami.

([1]) Motyw 20 i art. 3 ust. 3 i 5 wniosku.

([2]) Zob. w tej kwestii art. 15 ust. 1 dyrektywy 95/46/WE. Dyrektywa ta zabrania podejmowania opartych wyłącznie na zautomatyzowanym przetwarzaniu danych decyzji mających istotny wpływ na daną osobę. W odniesieniu do kontekstu wniosku decyzje w ramach ochrony porządku publicznego w każdym przypadku mogą istotnie wpłynąć na osobę, której dotyczą dane. Także poddanie kolejnym kontrolom może mieć wpływ na osobę, której dotyczą dane, szczególnie jeżeli takie kontrole powtarzają się.

([3]) Zob. zwłaszcza opinia nr 5/2007 z dnia 17 sierpnia 2007 r. w sprawie Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych zawartej w lipcu 2007 r., WP 138.

([4]) Ocena skutków, załącznik A, „Metody przekazywania danych przez przewoźników".

100. EIOD wyraża wątpliwości co do różnicy między tymi dwoma rodzajami baz danych: jest wątpliwe, czy archiwalna baza danych stanowi rzeczywiste archiwum, umożliwiające korzystanie z różnych metod przechowywania i wyszukiwania danych. Większość warunków, jakimi obwarowany jest dostęp do archiwalnej bazy danych, to wymagania dotyczące bezpieczeństwa, które mogłyby mieć zastosowanie również do bazy służącej do pięcioletniego przechowywania danych.

101. Całkowity okres przechowywania danych — wynoszący 13 lat — w każdym przypadku jest zbyt długi. W ocenie skutków regulacji uzasadniono go potrzebą opracowania wskaźników ryzyka i określeniem wzorców w zakresie tras podróży i zachowań ([1]), których skuteczność wymaga dowiedzenia. Choć jest oczywiste, że dane można przechowywać tak długo, jak to potrzebne, póki prowadzone jest dochodzenie w konkretnej sprawie, nie ma możliwego uzasadnienia dla zatrzymywania przez 13 lat danych wszystkich pasażerów przy absolutnym braku podejrzeń wobec nich.

102. EIOD ponadto zauważa, że ta długość okresu przechowywania danych nie została poparta przez państwa członkowskie w odpowiedziach udzielonych w związku z rozesłanym przez Komisję kwestionariuszem; zgodnie z tymi odpowiedziami przeciętny wymagany okres przechowywania danych wynosiłby 3,5 roku ([2]).

103. Co więcej, 13-letni okres przechowywania jest porównywalny z okresem 15-letnim ustalonym w najnowszej umowie ze Stanami Zjednoczonymi. EIOD jak dotąd uważał, że wyrażono zgodę na tak długi okres przechowywania danych tylko ze względu na silne naciski ze strony rządu USA, by był on znacząco dłuższy niż 3,5 roku, nie zaś ze względu na poparcie go na jakimkolwiek etapie przez Radę lub Komisję. Nie ma powodu, by transponować to zobowiązanie — uzasadnione jedynie wynikiem negocjacji — do aktu prawnego w obrębie samej UE.

Rola komitetu przedstawicieli państw członkowskich

104. Komitet przedstawicieli państw członkowskich ustanowiony na mocy art. 14 wniosku będzie posiadał kompetencje w zakresie bezpieczeństwa, w tym protokołów i standardów szyfrowania danych PNR, a także w zakresie wspólnych ogólnych kryteriów, metod i praktyk przeprowadzania oceny zagrożenia.

105. Poza tymi wskazówkami wniosek nie zawiera żadnych elementów ani kryteriów odnoszących się do konkretnych warunków i ram przeprowadzania oceny zagrożenia. W ocenie skutków regulacji wspomniano, że kryteria będą ostatecznie zależały od informacji wywiadowczych posiadanych przez każde państwo członkowskie, które podlegają ciągłej ewolucji. Ma się przeprowadzać oceny zagrożenia przy braku jednolitych standardów identyfikacji podejrzanych. Zakres, w jakim komitet przedstawicieli państw członkowskich będzie w stanie odgrywać jakąkolwiek rolę w tym procesie, budzi zatem wątpliwości.

Zabezpieczenie

106. We wniosku szczegółowo omówiono pewną liczbę środków bezpieczeństwa ([3]), jakie biura danych pasażerów, pośrednicy i inne właściwe organy mają podejmować w celu ochrony danych. Biorąc pod uwagę znaczenie tej bazy danych i wrażliwość procesu przetwarzania, EIOD uważa, że poza przewidzianymi środkami podmiot przetwarzający dane powinien być również zobowiązany do oficjalnego powiadamiania o naruszeniach bezpieczeństwa.

107. EIOD jest świadomy, że istnieje projekt ustanowienia takiej procedury powiadamiania na szczeblu europejskim w sektorze łączności elektronicznej. Radzi zatem, by włączyć takie zabezpieczenie do omawianego wniosku i odnosi się w tym względzie do systemu naruszeń bezpieczeństwa zastosowanego w Stanach Zjednoczonych w odniesieniu do agencji rządowych ([4]). Incydenty związane z naruszeniem bezpieczeństwa mogą mieć miejsce w jakiejkolwiek dziedzinie działalności, zarówno w sektorze prywatnym, jak i publicznym, jak pokazuje niedawna utrata całej bazy danych obywateli przez administrację brytyjską ([5]). Wielkoskalowe bazy danych takie, jak baza przewidziana w omawianym wniosku, odniosłyby największe korzyści z systemu powiadamiania.

Klauzule przeglądu i wygaśnięcia

108. EIOD odnotowuje, że w terminie trzech lat od wejścia decyzji ramowej w życie ma zostać przeprowadzony przegląd tej decyzji na podstawie sprawozdania przygotowanego przez Komisję. EIOD przyjmuje do wiadomości, że ten przegląd, oparty na informacjach przekazanych przez państwa członkowskie, skupi się szczególnie na środkach ochrony danych oraz obejmie wdrożenie metody dostarczania danych, ich zatrzymywania oraz jakości oceny zagrożenia. Aby taki przegląd objął wszystkie niezbędne aspekty, powinien obejmować wyniki analizy danych statystycznych wynikających z przetwarzania danych PNR. Te dane statystyczne, poza elementami wspomnianymi w art. 18 wniosku, powinny obejmować szczegółowe dane dotyczące ustalenia tożsamości osób stanowiących zagrożenie, takie jak kryteria identyfikacji oraz konkretne wyniki wszelkich działań związanych z ochroną porządku publicznego podejmowanych w wyniku identyfikacji osoby.

([1]) Ocena skutków, załącznik A, „Okres przechowywania danych".
([2]) Ocena skutków, załącznik B.
([3]) Artykuł 12 wniosku.
([4]) Zob. zwłaszcza opracowania amerykańskiego „Identity Theft Task Force":
http://www.idtheft.gov/
([5]) Zob. strona internetowa brytyjskich organów podatkowych i celnych (British HM Revenue and Customs):
http://www.hmrc.gov.uk/childbenefit/update-faqs.htm
Zob. także:
http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

109. EIOD podkreślił już w niniejszej opinii brak konkretnych elementów umożliwiających stwierdzenie konieczności wprowadzenia omawianego systemu. Uważa jednak, że — o ile decyzja ramowa wejdzie w życie — należy ją co najmniej uzupełnić o klauzulę wygaśnięcia. Na koniec trzyletniego okresu decyzję ramową należy uchylić, jeżeli brak będzie elementów przemawiających za jej dalszym obowiązywaniem.

Wpływ na inne instrumenty prawne

110. W przepisach końcowych wniosku zawarto warunek dotyczący dalszego stosowania już obowiązujących umów lub uzgodnień dwu- i wielostronnych. Instrumenty te mogą być stosowane wyłącznie, jeżeli są zgodne z celami proponowanej decyzji ramowej.

111. EIOD ma wątpliwości co do zakresu tego przepisu. Jak wspomniano w rozdziale V poświęconym wzajemności, nie jest jasne, jaki będzie wpływ tego przepisu na treść umów z państwami trzecimi, takich jak umowa z USA. Z innej perspektywy, nie jest też jasne, czy przepis ten mógłby wpływać na warunki stosowania instrumentów o szerszym zakresie, takich jak konwencja Rady Europy nr 108. Należy unikać wszelkiego ryzyka niewłaściwej interpretacji, niezależnie od tego, jak mało wydaje się ono prawdopodobne ze względu na różnice kontekstu instytucjonalnego i różnice między zaangażowanymi podmiotami, a wniosek powinien jasno stwierdzać, że nie ma wpływu na instrumenty o szerszym zakresie zastosowania, przede wszystkich te mające na celu ochronę praw podstawowych.

VII. **PODSUMOWANIE**

112. EIOD podkreśla znaczący wpływ omawianego wniosku na ochronę danych. Analiza została poświęcona przede wszystkim czterem zasadniczym kwestiom zawartym we wniosku; EIOD podkreśla, że kwestie te wymagają kompleksowego podejścia. W obecnych warunkach wniosek nie jest zgodny z prawami podstawowymi, przede wszystkim z art. 8 Karty Praw Podstawowych Unii Europejskiej, i nie powinien zostać przyjęty.

113. W przypadku uwzględnienia powyższych uwag, szczególnie dotyczących sprawdzenia zgodności z prawem, w niniejszej opinii zawarto kilka propozycji zmiany tekstu, które powinny zostać uwzględnione przez prawodawcę. Zwraca się uwagę zwłaszcza na pkt 67, 73, 77, 80, 90, 93, 106, 109 i 111 niniejszej opinii.

Zgodność proponowanych działań z prawem

114. Choć ogólny cel polegający na walce z terroryzmem i przestępczością zorganizowaną sam w sobie jest jasny i zgodny z prawem, najważniejsze elementy przetwarzania danych, które ma być realizowane, nie zostały wystarczająco dobrze określone ani uzasadnione.

115. EIOD uważa, że należy lepiej ocenić techniki polegające na ocenie zagrożenia, jakie stanowią poszczególne osoby, z wykorzystaniem narzędzi eksploracji danych i wzorców zachowania; należy również jasno określić ich użyteczność w ramach walki z terroryzmem, zanim zaczną być stosowane na szeroką skalę.

116. Opieranie się na różnych bazach danych bez globalnej perspektywy konkretnych wyników i niedociągnięć:

— sprzeciwia się racjonalnej polityce prawodawczej, zgodnie z którą nie należy przyjmować nowych instrumentów, zanim instrumenty istniejące nie zostały w pełni wdrożone i nie dowiedziono ich nieskuteczności,

— mogłoby prowadzić do całkowitego nadzoru nad społeczeństwem.

117. Walka z terroryzmem z całą pewnością może stanowić uzasadnienie dla zastosowania wyjątków od podstawowych praw do prywatności i ochrony danych. By jednak uzasadnienie to było ważne, konieczność ingerencji musi być poparta jasnymi i niezaprzeczalnymi dowodami; należy też dowieść proporcjonalności przetwarzania danych. Jest to tym bardziej konieczne w przypadku tak szerokiej ingerencji w prywatność poszczególnych osób, jaką przewidziano we wniosku.

118. We wniosku brak jest tych elementów uzasadnienia; nie sprawdzono też konieczności przyjęcia wniosku i jego proporcjonalności.

119. EIOD podkreśla, że testy konieczności i proporcjonalności są kwestią podstawową. Stanowią one *condicio sine qua non* wejścia omawianego wniosku w życie.

Ramy prawne mające zastosowanie

120. EIOD zauważa poważny brak pewności prawnej w odniesieniu do systemu ochrony danych mającego zastosowanie do różnych podmiotów uczestniczących w przedsięwzięciu, a szczególnie linii lotniczych i innych podmiotów należących do pierwszego filaru: niezależnie od tego, czy chodzi o przepisy wniosku, przepisy decyzji ramowej o ochronie danych czy ustawodawstwo krajowe wdrażające dyrektywę 95/46/WE. Prawodawca powinien wyjaśnić, na których etapach przetwarzania danych będą miały zastosowanie te różne przepisy.

121. Obecna tendencja do systematycznego nakładania na podmioty prywatne obowiązku współpracy z organami ochrony porządku publicznego, co wiąże się z pytaniem, które ramy ochrony danych (należące do pierwszego czy trzeciego filaru) mają zastosowanie do warunków tej współpracy: nie jest jasne, czy przepisy powinny być oparte na cechach administratora danych (sektor prywatny) czy na celu, który ma zostać osiągnięty (ochrona porządku publicznego).

122. EIOD wcześniej podkreślił ryzyko luki prawnej między działaniami w ramach pierwszego i trzeciego filaru ([1]). Rzeczywiście nie jest jasne, które działania firm prywatnych, w pewien sposób związane z egzekwowaniem prawa karnego, są objęte zakresem działania prawodawcy Unii Europejskiej na mocy art. 30, 31 i 34 Traktatu UE.

123. Należy zatem unikać sytuacji, której rezultatem byłoby objęcie przetwarzania danych przez dostawców usług różnymi ramami ochrony danych w zależności od celu przetwarzania, zwłaszcza biorąc pod uwagę trudności, jakie stworzyłoby to dla korzystania przez osoby, których dotyczą dane, ze swoich praw.

Charakter odbiorców danych

124. Wniosek powinien przewidywać specyfikację cech odbiorców danych osobowych gromadzonych przez linie lotnicze, czy to dla pośredników, czy też dla biur danych pasażerów lub właściwych organów.

125. Charakter odbiorcy danych, który w pewnych przypadkach może należeć do sektora prywatnego, jest bezpośrednio związany z rodzajem gwarancji dotyczących ochrony danych, które mają zastosowanie do tego odbiorcy. Kwestią zasadniczą jest, by mający zastosowanie system był jasny dla wszystkich zainteresowanych podmiotów, w tym prawodawcy, organów ochrony danych oraz administratorów danych i osób, których te dane dotyczą.

Transfer danych do państw trzecich

126. EIOD podkreśla potrzebę zapewnienia właściwego poziomu ochrony w kraju przyjmującym dane. Ma również wątpliwości co do znaczenia zasady „wzajemności" wspomnianej we wniosku oraz jej zastosowania do krajów już związanych umową z UE, jak Kanada lub USA. Uważa za kwestię kluczową spójność warunków przekazywania danych PNR do państw trzecich oraz podleganie tych warunków ujednoliconemu poziomowi ochrony.

Inne zastrzeżenia merytoryczne

127. EIOD zwraca uwagę prawodawcy na konkretne aspekty wniosku, które wymagają doprecyzowania lub lepszego uwzględnienia zasady ochrony danych. W szczególności chodzi o następujące aspekty:

— ograniczenie warunków, na jakich mogą być podejmowane decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu danych,

— zmniejszenie ilości przetwarzanych danych,

— metodę transferu danych, która powinna zostać oparta wyłącznie na ich dostarczaniu,

— okres przechowywania danych uznany za zbyt długi i nieuzasadniony,

— sprecyzowanie roli komitetu przedstawicieli państw członkowskich w odniesieniu do udzielania wskazówek dotyczących oceny zagrożenia,

— uwzględnienie wśród środków bezpieczeństwa procedury powiadamiania o naruszeniach bezpieczeństwa,

— włączenie do przeglądu decyzji klauzuli wygaśnięcia,

— wyjaśnienie we wniosku, że nie ma on wpływu na instrumenty o szerszym zakresie zastosowania mające na celu ochronę praw podstawowych.

Uwagi końcowe

128. EIOD przyjmuje do wiadomości, że omawiany wniosek został złożony w chwili, w której kontekst instytucjonalny Unii Europejskiej ma ulec zasadniczym zmianom. Konsekwencje traktatu lizbońskiego dla procedury decyzyjnej, a szczególnie roli Parlamentu, są fundamentalne.

129. Biorąc pod uwagę bezprecedensowy wpływ omawianego wniosku na kwestie praw podstawowych, EIOD radzi nie przyjmować go na podstawie obowiązujących traktatów, lecz zapewnić jego przyjęcie w ramach procedury współdecyzji przewidzianej w nowym traktacie. Wzmocniłoby to podstawy prawne, na których podejmowane byłyby najważniejsze środki przewidziane we wniosku.

([1]) Zob. opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji dla Parlamentu Europejskiego i Rady w sprawie kontynuacji programu prac na rzecz skuteczniejszego wdrażania dyrektywy o ochronie danych (Dz.U. C 255 z 27.10.2007, str. 1). Zob. także sprawozdanie roczne za 2006 r., str. 47.