I

(Rezolucje, zalecenia i opinie)

OPINIE

EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych w sprawie sprawozdania końcowego grupy kontaktowej wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych

(2009/C 128/01)

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,

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, w szczególności jego art. 41,

WYDAJE NASTĘPUJĄCĄ OPINIĘ:

I. **WPROWADZENIE – KONTEKST OPINII**

1. W dniu 28 maja 2008 r. prezydencja Rady Unii Europejskiej – z myślą o szczycie UE zaplanowanym na 12 czerwca 2008 r. – przekazała COREPER-owi informację o tym, że grupa kontaktowa wysokiego szczebla UE–USA ds. wymiany informacji oraz ochrony prywatności i danych osobowych (zwana dalej „grupą kontaktową") ostatecznie zakończyła prace nad swoim sprawozdaniem. W dniu 26 czerwca 2008 r. sprawozdanie to zostało podane do wiadomości publicznej [1].

2. W sprawozdaniu starano się wskazać wspólne zasady, którym podlegałaby ochrona prywatności i danych, a tym samym poczynić pierwszy krok ku wymianie informacji między UE a USA w celu walki z terroryzmem i z poważną przestępczością międzynarodową.

3. W swoim oświadczeniu prezydencja Rady zakomunikowała, że oczekuje na wszelkie pomysły co do realizacji sprawozdania, a zwłaszcza na opinie o zawartych w nim zaleceniach na temat dalszych działań. Wydając niniejszą opinię, Inspektor odpowiada na to zaproszenie; opiera się przy tym na upublicznionych informacjach o stanie prac i zastrzega możliwość zabrania głosu także później, jeżeli prace te będą się rozwijać.

4. Inspektor odnotowuje, że prace grupy kontaktowej toczyły się w sytuacji, gdy – zwłaszcza po dniu 11 września 2001 r. – dzięki umowom międzynarodowym lub innym rodzajom aktów rozwijała się wymiana danych pomiędzy USA i UE. Wśród wspomnianych umów i innych aktów należy wymienić umowy Europolu i Eurojustu z USA, umowy w sprawie danych o przelocie pasażera (PNR), a także sprawę SWIFT, która zaowocowała wymianą listów pomiędzy przedstawicielami UE i USA służącą ustanowieniu minimalnych gwarancji ochrony danych [2].

[1] Dokument Rady nr 9831/08, dostępny pod adresem: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

[2] — Umowa z dnia 6 grudnia 2001 r. pomiędzy Stanami Zjednoczonymi Ameryki a Europejskim Urzędem Policji oraz Dodatkowa umowa pomiędzy Europolem a USA w sprawie wymiany danych osobowych i informacji pokrewnych (opublikowana na stronie internetowej Europolu);
— Umowa z dnia 6 listopada 2006 r. pomiędzy Stanami Zjednoczonymi Ameryki a Eurojustem w sprawie współpracy sądowej (opublikowana na stronie internetowej Eurojustu);
— 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 (DHS) (umowa PNR z 2007 r.), podpisana w Brukseli w dniu 23 lipca 2007 r. i w Waszyngtonie w dniu 26 lipca 2007 r. (Dz.U. L 204 z 4.8.2007, s. 18);
— Wymiana listów z dnia 28 czerwca 2007 r. pomiędzy władzami USA i UE w sprawie programu śledzenia środków finansowych należących do terrorystów.

5. Ponadto UE negocjuje i zatwierdza podobne akty przewidujące wymianę danych osobowych z innymi krajami trzecimi. Ostatnim tego przykładem jest Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej danych dotyczących przelotu pasażera (danych PNR) pochodzących z Unii Europejskiej ([3]).

6. Wynika z tego, że zapotrzebowanie organów ochrony porządku publicznego z krajów trzecich na dane osobowe wciąż rośnie i oprócz tradycyjnych rządowych baz danych zaczyna obejmować także innego rodzaju rejestry, zwłaszcza takie, w których znajdują się dane zgromadzone przez sektor prywatny.

7. Inspektor chciałby zwrócić uwagę na jeszcze jedną ważną kwestię, a mianowicie na to, że problem przekazywania danych osobowych do krajów trzecich w ramach współpracy policyjnej i sądowej w sprawach karnych poruszono także w decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych ([4]); decyzja ta powinna zostać przyjęta jeszcze w 2008 r.

8. Należy się spodziewać, że transatlantycka wymiana informacji będzie rosła i obejmie kolejne sektory, w których przetwarza się dane osobowe. W tej sytuacji rozmowy o „transatlantyckim egzekwowaniu prawa" są potrzebne, a jednocześnie trudne. Są potrzebne w tym sensie, że mogą skutkować bardziej przejrzystymi przepisami prawnymi o wymianie danych, która już się odbywa lub będzie się odbywać w przyszłości. Są także trudne, ponieważ takie przepisy mogłyby umożliwić masowe przekazywanie danych w sektorze egzekwowania prawa, którego wpływ na obywateli jest wyjątkowo poważny, a więc w którym tym bardziej muszą obowiązywać ścisłe i niezawodne zabezpieczenia i gwarancje ([5]).

9. W następnym rozdziale niniejszej opinii skoncentrowano się na obecnym stanie prac i na możliwościach dalszych działań. W rozdziale III skupiono się na zakresie i charakterze aktu, który pozwoli wymieniać się informacjami. W rozdziale IV rozpatrzono – z ogólnego punktu widzenia – kwestie prawne związane z treścią ewentualnej umowy. Poruszono takie sprawy jak warunki pomagające ocenić gwarantowany przez USA stopień ochrony danych oraz omówiono stosowanie unijnych ram regulacyjnych jako punktu odniesienia pozwalającego ocenić wspomniany stopień ochrony danych. W rozdziale tym zamieszczono także wykaz podstawowych wymogów, które należy zawrzeć w takiej umowie. Natomiast w rozdziale V przeanalizowano załączone do sprawozdania zasady rządzące prywatnością.

([3]) Dz.U. L 213 z 8.8.2008, s. 49.

([4]) Decyzja ramowa Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, wersja z dnia 24 czerwca 2008 r. dostępna pod adresem: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=pl&DosId=193371

([5]) Jeżeli chodzi o potrzebę stworzenia przejrzystych przepisów prawnych, zob. rozdział III i IV niniejszej opinii.

II. OBECNY STAN PRAC I MOŻLIWOŚCI DALSZYCH DZIAŁAŃ

10. Inspektor ocenia obecny stan prac następująco: osiągnięto pewne postępy w wypracowywaniu definicji wspólnych norm wymiany informacji oraz ochrony prywatności i danych osobowych.

11. Jednak prace przygotowawcze zmierzające do opracowania dowolnego rodzaju umowy pomiędzy UE a USA jeszcze się nie zakończyły. Potrzeba dodatkowych wysiłków. Już w samym sprawozdaniu grupy kontaktowej wskazano kilka nierozstrzygniętych kwestii, z których najważniejszą jest sprawa środków odwoławczych. Nie porozumiano się jeszcze co do niezbędnego zakresu sądowych środków odwoławczych ([6]). W rozdziale 3 sprawozdania wymieniono jeszcze pięć innych nierozstrzygniętych kwestii. Ponadto z niniejszej opinii wynika, że nie rozwiązano jeszcze wielu innych problemów, np. tego, jaki zakres i charakter ma mieć akt dotyczący wymiany informacji.

12. Ponieważ w sprawozdaniu za pożądaną opcję uznano wiążącą umowę – a Inspektor podziela tę opinię – tym bardziej potrzeba rozwagi. Zanim dojdzie do porozumienia, należy przeprowadzić dalsze uważne i dogłębne przygotowania.

13. Ponadto, zdaniem Inspektora, najlepiej, gdyby do zawarcia umowy doszło, gdy obowiązywać będzie Traktat Lizboński – o ile oczywiście wejdzie on w życie. W jego przypadku nie ma wątpliwości co do rozgraniczenia między poszczególnymi filarami UE, a zatem sprzyja on pewności prawa. Ponadto zagwarantuje pełne zaangażowanie ze strony Parlamentu Europejskiego oraz kontrolę sądową ze strony Trybunału Sprawiedliwości.

14. W tej sytuacji najlepszym sposobem dalszych działań byłoby przygotowanie planu prac, który prowadziłby do sporządzenia umowy na późniejszym etapie. Taki plan mógłby zawierać następujące elementy:

— Wskazówki dla grupy kontaktowej (lub innej grupy) co do dalszych prac i ich harmonogram.

— Na początkowym etapie: rozmowy i ewentualne porozumienie co do podstawowych kwestii, takich jak zakres i charakter przedmiotowej umowy.

— Dalsze wypracowywanie – na podstawie porozumienia co do podstawowych kwestii – zasad rządzących ochroną danych.

— Włączanie zainteresowanych stron w prace na poszczególnych etapach.

— Ze strony europejskiej – przeciwdziałanie ograniczeniom instytucjonalnym.

([6]) Strona 5 sprawozdania, pkt C.

III. ZAKRES I CHARAKTER AKTU POŚWIĘCONEGO WYMIANIE INFORMACJI

15. Inspektor sądzi, że niezwykle ważne jest, by w pierwszej kolejności wyraźnie zdefiniować zakres i charakter ewentualnego aktu, w tym zasady rządzące ochroną danych, ponieważ pozwoli to następnie dalej go rozwijać.

16. Jeżeli chodzi o zakres aktu, należy odpowiedzieć na następujące istotne pytania:

— których podmiotów z sektora egzekwowania prawa i spoza niego akt ten ma dotyczyć;

— co należy rozumieć pod pojęciem „cele związane z egzekwowaniem prawa" i jaki ma ono związek z innymi celami, takimi jak bezpieczeństwo narodowe, a konkretnie kontrola graniczna i zdrowie publiczne;

— w jaki sposób akt ten wpisywałby się w ideę globalnego transatlantyckiego obszaru bezpieczeństwa.

17. Definiując charakter aktu, należy sprecyzować następujące kwestie:

— w odpowiednim przypadku – w ramach którego filaru UE negocjowany będzie przedmiotowy akt;

— czy akt ten będzie dla UE i USA wiążący;

— czy będzie miał bezpośrednie zastosowanie, to znaczy czy będzie przyznawał osobom fizycznym prawa i nakładał na nie obowiązki, które będzie można egzekwować przed sądem;

— czy sam akt będzie umożliwiał wymianę informacji, czy raczej ustanowi minimalne normy tej wymiany i zostanie uzupełniony umowami szczegółowymi;

— jaki będzie stosunek tego aktu do aktów już obowiązujących: czy będzie je respektował, czy je zastąpi, czy uzupełni?

III.1. Zakres aktu

Zaangażowane podmioty

18. Choć w sprawozdaniu grupy kontaktowej nie powiedziano wyraźnie, jaki zakres miałby dokładnie mieć przyszły akt, z zasad, o których mowa w tym dokumencie, można wywnioskować, że ma objąć przekazywanie danych zarówno między podmiotami prywatnymi a publicznymi ([7]), jak i między władzami publicznymi.

— Między podmiotami prywatnymi a publicznymi:

19. Inspektor dostrzega logikę przemawiającą za zastosowaniem przyszłego aktu do przekazywania danych między podmiotami prywatnymi a publicznymi. Dokument ten jest opracowywany, ponieważ w ostatnich latach z USA nadchodzą prośby o udostępnianie informacji przez podmioty prywatne. Inspektor odnotowuje, że podmioty prywatne faktycznie coraz częściej stają się źródłem informacji przeznaczonych do celów egzekwowania prawa – zarówno na szczeblu UE, jak i na szczeblu międzynarodowym ([8]). Ważny precedens stanowiła sprawa SWIFT, kiedy to prywatne przedsiębiorstwo zostało poproszone o systematyczne przekazywanie hurtowej ilości danych organom ochrony porządku publicznego z kraju trzeciego ([9]). Ta sama logika przemawia za gromadzeniem danych o przelocie pasażera od linii lotniczych. Jednak już w opinii na temat projektu decyzji ramowej o europejskim systemie takich danych Inspektor zakwestionował zgodność tych działań z prawem ([10]).

20. Istnieją jeszcze dwa inne powody, dla których objęcie przyszłym aktem przekazywania danych między podmiotami prywatnymi a publicznymi budzi wątpliwości.

21. Po pierwsze, działanie takie może przynieść niepożądane skutki na terytorium samej UE. Inspektor ma poważne obawy, że jeśli dane pochodzące od prywatnych przedsiębiorstw (np. instytucji finansowych) z zasady będą mogły być przekazywane krajom trzecim, spowoduje to poważną presję, by tego samego rodzaju dane były również udostępniane organom ochrony porządku publicznego w UE. Przykładem takiego niepożądanego następstwa wydarzeń jest system danych o przelocie pasażera, który rozpoczął się od hurtowego gromadzenia danych pasażerów przez USA, a następnie został przeniesiony na wewnętrzny europejski grunt ([11]), choć nie wykazano wyraźnie potrzeby ani adekwatności takiego systemu.

22. Po drugie, w opinii na temat wniosku Komisji w sprawie europejskiego systemu danych o przelocie pasażera Inspektor poruszył także problem tego, które przepisy prawne (pierwszy czy trzeci filar) należy stosować, określając warunki współpracy miedzy podmiotami publicznymi a prywatnymi: czy reguły powinny zależeć od cech administratora danych (sektor prywatny) czy od wyznaczonego celu (egzekwowanie prawa)? Rozgraniczenie między

([7]) Zob. przede wszystkim rozdział 3 sprawozdania: „Nierozstrzygnięte kwestie dotyczące stosunków transatlantyckich", pkt 1: „Spójność obowiązków, którym podlegają podmioty prywatne podczas przekazywania danych".

([8]) Por. w tej sprawie: opinia Europejskiego Inspektora Ochrony Danych z dnia 20 grudnia 2007 r. w sprawie projektu wniosku dotyczącego decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa (Dz.U. C 110 z 1.5.2008, s. 1). „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".

([9]) Zob. opinia Grupy Roboczej Art. 29 10/2006 z dnia 22 listopada 2006 r. w sprawie przetwarzania danych osobowych przez Stowarzyszenia na rzecz Światowej Międzybankowej Telekomunikacji Finansowej (SWIFT), WP 128.

([10]) Opinia z dnia 20 grudnia 2007 r., op. cit.

([11]) Zob. wspomniany w przypisie 8 wniosek dotyczący decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu egzekwowania prawa (obecnie omawiany na forum Rady).

pierwszym a trzecim filarem nie jest jasne w sytuacjach, gdy na podmioty prywatne nakłada się obowiązek przetwarzania danych osobowych do celów egzekwowania prawa. Znaczący w tym kontekście jest fakt, że rzecznik generalny Yves Bot w swojej niedawnej opinii w sprawie zatrzymywania danych ([12]) proponuje rozgraniczyć te sytuacje, ale dodaje: „Taka linia demarkacyjna nie jest oczywiście przyjmowana w pełni bezkrytycznie i może się pod pewnymi względami wydawać sztuczna". Inspektor odnotowuje również, że wyrok Trybunału w sprawie danych o przelotach pasażera ([13]) nie daje pełnej odpowiedzi na pytanie o stosowne przepisy prawne. Na przykład fakt, że niektóre działania nie są objęte dyrektywą 95/46/WE nie oznacza automatycznie, że mogą być regulowane w ramach trzeciego filaru. W efekcie wyrok prawdopodobnie pozostawia lukę co do tego, które prawodawstwo należy stosować, a w każdym razie sprzyja niepewności prawa, jeżeli chodzi o gwarancje prawne przysługujące osobom, których dane dotyczą.

23. W związku z powyższym Inspektor zwraca uwagę, że należy dopilnować, by przyszły akt, zawierający ogólne zasady ochrony danych, nie legitymizował jako takiego transatlantyckiego przekazywania danych osobowych między podmiotami prywatnymi a publicznymi. O takim przekazywaniu danych przyszły akt może mówić tylko wtedy, gdy:

— będzie przewidywał, że jest ono możliwe wyłącznie w sytuacji, gdy udowodni się, że jest ono absolutnie niezbędne do konkretnych celów, i gdy będzie rozpatrywane dla każdego przypadku z osobna,

— przekazywaniu danych towarzyszyć będą ścisłe zabezpieczenia (opisane w niniejszej opinii).

Ponadto Inspektor zwraca uwagę, że istnieje niepewność co do stosownych przepisów prawnych o ochronie danych, i dlatego apeluje, by w żadnym wypadku nie przewidywać w umowie przekazywania danych osobowych między podmiotami prywatnymi a publicznymi na mocy obecnie obowiązującego prawa UE.

— Między władzami publicznymi:

24. Niejasny jest dokładny zakres wymiany informacji. Podczas dalszych prac zmierzających do sporządzenia wspólnego aktu należy w pierwszej kolejności sprecyzować jego planowany zakres. Wątpliwości budzi przede wszystkim to, czy:

— jeżeli chodzi o bazy danych znajdujące się w UE, akt miałby dotyczyć scentralizowanych baz (częściowo) administrowanych przez UE, takich jak baza danych Europolu i baza danych Eurojustu, zdecentralizowanych baz administrowanych przez państwa członkowskie, czy obu tych rodzajów baz;

— akt miałby dotyczyć także sieci połączonych, tzn. czy przewidywanymi gwarancjami miałyby zostać objęte dane wymieniane przez państwa członkowskie lub przez agencje w UE i w USA;

— akt miałby objąć tylko wymianę między bazami danych z sektora egzekwowania prawa (policja, wymiar sprawiedliwości, ewentualnie służby celne) czy również między innymi bazami danych, np. podatkowymi;

— akt miałby się odnosić również do baz danych należących do krajowych agencji bezpieczeństwa oraz czy dawałby tym agencjom dostęp do baz danych służących egzekwowaniu prawa i znajdujących się na terytorium drugiej strony (UE na terytorium USA i odwrotnie);

— akt przewidywałby przekazywanie informacji w pojedynczych przypadkach czy raczej stały dostęp do istniejących baz danych. Ta ostatnia hipoteza bez wątpienia sprzyjałaby pytaniom o proporcjonalność, które omówiono w rozdziale V pkt 3.

Cel „egzekwowanie prawa"

25. Zdefiniowany cel ewentualnej umowy również pozostawia pewne wątpliwości. O celach związanych z egzekwowaniem prawa wyraźnie wspomniano we wprowadzeniu do przedmiotowego sprawozdania oraz w omówieniu pierwszej załączonej zasady; zostaną one dokładniej przeanalizowane w rozdziale IV niniejszej opinii. Inspektor już teraz zwraca uwagę, że ze stwierdzeń tych wynika, iż wymiana danych będzie dotyczyć głównie spraw objętych trzecim filarem, ale można się zastanawiać, czy nie jest to pierwszy krok do szerszej wymiany informacji. Wydaje się jasne, że wspomniane w sprawozdaniu cele z zakresu „bezpieczeństwa publicznego" to między innymi walka z terroryzmem, przestępczością zorganizowaną i innymi przestępstwami. Czy oznacza to jednak, że dopuszczalna byłaby wymiana danych w innego rodzaju interesie publicznym, np. w przypadku zagrożeń dla zdrowia publicznego?

26. Inspektor zaleca, by ograniczyć cel umowy do dokładnie określonego przetwarzania danych i uznać za zasadne decyzje polityczne prowadzące do takiego zdefiniowania celu.

([12]) Opinia rzecznika generalnego Yves'a Bota z dnia 14 października 2008 r., Irlandia przeciwko Parlamentowi Europejskiemu i Radzie (sprawa C-301/06), pkt 108.

([13]) Wyrok Trybunału z dnia 30 maja 2006 r., Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), sprawy połączone C-317/04 i C-318/04, Zb. Orz. [2006], s. I-4721.

Globalny transatlantycki obszar bezpieczeństwa

27. Szeroki zakres przedmiotowego sprawozdania należy interpretować w powiązaniu z problemem globalnego transatlantyckiego obszaru bezpieczeństwa – tematem omawianym przez tzw. grupę ds. przyszłości ([14]). Sprawozdanie tej grupy, wydane w czerwcu 2008 r., kładzie pewien nacisk na zewnętrzny wymiar polityki wewnętrznej. Mówi ono, że „do roku 2014 Unia Europejska powinna się także określić co do politycznego celu, jakim byłoby stworzenie euro-atlantyckiej przestrzeni współpracy z USA w dziedzinie wolności, bezpieczeństwa i sprawiedliwości". Taka współpraca wykroczyłaby poza sprawy bezpieczeństwa sensu stricto i objęłaby kwestie podlegające obecnie tytułowi IV Traktatu WE, takie jak imigracja, wizy i azyl oraz współpraca w dziedzinie prawa cywilnego. Należy zadać pytanie, do jakiego stopnia umowa w sprawie podstawowych zasad ochrony danych, takich jak zasady wymienione w sprawozdaniu grupy kontaktowej, może i powinna służyć za podstawę do wymiany informacji w tak szerokiej dziedzinie.

28. W normalnych warunkach do 2014 roku struktura filarowa przestanie istnieć, a ochrona danych w UE będzie mieć jedną podstawę prawną (na mocy traktatu lizbońskiego: art. 16 Traktatu o funkcjonowaniu Unii Europejskiej). Jednak fakt, że na szczeblu UE obowiązuje harmonizacja *przepisów* o ochronie danych, nie oznacza, że jakakolwiek umowa z krajem trzecim miałby umożliwiać *przekazywanie* jakichkolwiek danych osobowych do jakichkolwiek celów. Zależnie od kontekstu i warunków przetwarzania danych, w określonych dziedzinach, takich jak egzekwowanie prawa, potrzebne mogą być specjalnie dostosowane gwarancje ochrony danych. Inspektor zaleca, by podczas opracowywania przyszłej umowy wziąć pod uwagę skutki ewentualnych przyszłych zmian.

III.2. **Charakter umowy**

Europejskie ramy instytucjonalne

29. Najpierw należy przede wszystkim określić, w ramach którego filaru negocjowana będzie umowa. Jest to niezbędne, ponieważ umowa taka będzie miała wpływ na wewnętrzne ramy regulacyjne dotyczące ochrony danych. Czy będą to akty prawne podlegające pierwszemu filarowi – głównie dyrektywa 95/46/WE i jej specjalny system przekazywania danych do krajów trzecich – czy może akty podlegające trzeciemu filarowi i przewidujące mniej rygorystyczny system przekazywania danych do krajów trzecich ([15])?

30. Choć – jak już wspomniano – przeważają cele związane z egzekwowaniem prawa, jednak grupa kontaktowa w swoim sprawozdaniu wspomina o gromadzeniu danych od podmiotów prywatnych, a same cele można interpretować szeroko, odnosząc je nie tylko do samego bezpieczeństwa, np. do imigracji i kontroli granicznej, lecz także np. do zdrowia publicznego. W związku z tymi niejasnościami najlepiej byłoby poczekać na harmonizację filarów w prawie UE przewidzianą w traktacie lizbońskim i dopiero wtedy wyraźnie ustalić podstawę prawną negocjacji oraz dokładną rolę instytucji europejskich, zwłaszcza Parlamentu Europejskiego i Komisji.

Wiążący charakter aktu

31. Należy wyjaśnić, czy efektem rozmów będzie protokół ustaleń lub inny niewiążący akt, czy może wiążąca umowa międzynarodowa.

32. Inspektor podobnie jak autorzy sprawozdania opowiada się za wiążącą umową. Jego zdaniem oficjalna wiążąca umowa jest niezbędnym warunkiem tego, by jakiekolwiek dane mogły być przekazywane poza UE, bez względu na cel ich przekazywania. Nie można przekazywać danych do kraju trzeciego, jeżeli nie istnieje konkretny (i wiążący) akt prawny zawierający odpowiednie warunki i zabezpieczenia. Innymi słowy, protokół ustaleń lub inny niewiążący akt mogą być użyteczne jako wskazówka w negocjacjach nad dalszymi wiążącymi umowami, ale nigdy nie mogą takich umów zastąpić.

Bezpośredni skutek

33. Postanowienia aktu powinny być wiążące zarówno dla USA, jak i dla UE i jej państw członkowskich.

34. Należy ponadto dopilnować, by na podstawie uzgodnionych zasad osoby fizyczne mogły korzystać ze swoich praw, a zwłaszcza sięgać po środki odwoławcze. Inspektor jest zdania, że najlepiej byłoby w tym celu tak sformułować merytoryczne postanowienia aktu, by miały bezpośredni skutek wobec mieszkańców Unii Europejskiej i by można się było na nie powołać przed sądem. Dlatego też w akcie należy wyjaśnić, że postanowienia umowy międzynarodowej mają bezpośredni skutek i że zawiera ona warunki transpozycji aktu do wewnętrznego prawa europejskiego i krajowego, by zapewnić skuteczność środków.

Powiązania z innymi aktami

35. Zasadniczą kwestią jest także to, w jakim stopniu umowa ma być samodzielnym aktem, a w jakim powinna być uzupełniana – w pojedynczych przypadkach – dalszymi umowami dotyczącymi konkretnej wymiany danych. Wątpliwe jest, czy pojedyncza umowa mogłaby w dostateczny sposób, za pomocą jednego zbioru norm, objąć różnorodne specyficzne cechy przetwarzania danych w ramach trzeciego filaru. Jeszcze bardziej wątpliwe jest, czy powinna *dopuszczać* – bez dodatkowych rozmów i zabezpieczeń – ogólną zgodę na wszelkiego rodzaju przekazywanie danych osobowych, bez względu na cel tego

([14]) Sprawozdanie nieformalnej grupy doradczej wysokiego szczebla ds. przyszłości europejskiej polityki spraw wewnętrznych „Wolność, bezpieczeństwo, prywatność – europejskie sprawy wewnętrzne w otwartym świecie", czerwiec 2008, dostępne pod adresem: register.consilium.europa.eu

([15]) Zob. art. 11 i 13 decyzji ramowej, o której mowa w pkt 7 niniejszej opinii.

działania i na charakter danych. Poza tym umowy z krajami trzecimi niekoniecznie są zawierane na stałe, ponieważ mogą się wiązać z określonymi zagrożeniami, mogą podlegać przeglądowi, w tym przeglądowi wygaśnięcia. Z drugiej strony wspólne minimalne normy zatwierdzone w wiążącym akcie mogłyby sprzyjać dalszym rozmowom o przekazywaniu danych osobowych związanych z określonymi bazami danych lub z określonym procesem przetwarzania.

36. Dlatego Inspektor opowiada się raczej za minimalnymi kryteriami ochrony danych, które uzupełniano by w pojedynczych przypadkach o dodatkowe postanowienia szczegółowe, jak wspomniano w sprawozdaniu grupy kontaktowej, niż za samodzielną umową. Te dodatkowe postanowienia są wstępnym warunkiem, od którego zależałaby możliwość przekazania danych w konkretnym przypadku. Sprzyjałoby to zharmonizowanemu podejściu do ochrony danych.

Zastosowanie wobec obowiązujących aktów

37. Należy również przeanalizować, jak ewentualna umowa ogólna miałaby się do już obowiązujących umów między UE a USA. Należy zauważyć, że umowy te nie mają jednakowo wiążącego charakteru: wystarczy wspomnieć zwłaszcza umowę w sprawie danych o przelocie pasażera (dającą większą pewność prawa), umowy z Europolem i Eurojustem czy wymianę listów w sprawie SWIFT ([16]). Czy nowa umowa ogólna miałaby uzupełniać te akty czy raczej pozostawiłaby je nienaruszone, a stosowała się wyłącznie do przyszłej wymiany danych osobowych? Zdaniem Inspektora dla spójności prawa potrzebny byłby zharmonizowany zbiór reguł, który miałby zastosowanie zarówno do obowiązujących, jak i przyszłych wiążących umów o przekazywaniu danych i który by te umowy uzupełniał.

38. Zastosowanie umowy ogólnej do już obowiązujących aktów pozwoliłoby nadać im bardziej wiążący charakter. Byłoby to szczególnie pożądane w przypadku aktów, które nie są prawnie wiążące, np. wymiany listów w sprawie SWIFT, ponieważ nakładałoby przynajmniej obowiązek przestrzegania kilku ogólnych zasad odnoszących się do prywatności.

IV. **OGÓLNA OCENA PRAWNA**

39. W niniejszym rozdziale uwagę poświęcono temu, w jaki sposób ocenić stopień ochrony danych, który zapewniają określone przepisy prawne lub określony akt, w tym – jakie punkty odniesienia i jakie podstawowe wymogi stosować.

Odpowiedni stopień ochrony danych

40. Zdaniem Inspektora powinno być jasne, że przyszły akt ma dać przede wszystkim następujący efekt: przekazywanie danych osobowych do USA może mieć miejsce tylko wtedy, gdy władze tego kraju zapewnią odpowiedni stopień ich ochrony (i odwrotnie).

41. Inspektor sądzi, że o dostatecznym stopniu ochrony danych osobowych zaświadczyć może tylko faktyczna próba adekwatności. Uważa on, że ogólna umowa ramowa o zakresie tak szerokim, jak zaproponowano w sprawozdaniu grupy kontaktowej, mogłaby takiej próby nie przejść. Adekwatność umowy ogólnej można ocenić tylko w połączeniu z adekwatnością umów szczegółowych zawartych w pojedynczych przypadkach.

42. Ocena stopnia ochrony, jaki zapewniają kraje trzecie, nie jest niczym niezwykłym, zwłaszcza dla Komisji Europejskiej: w ramach pierwszego filaru odpowiedni stopień ochrony jest warunkiem przekazania danych. Kilkakrotnie oceniano go na mocy art. 25 dyrektywy 95/46 z użyciem konkretnych kryteriów i potwierdzano decyzjami Komisji Europejskiej ([17]). W ramach trzeciego filaru systemu takiego nie przewidziano wyraźnie: dokonywanie oceny, czy ochrona jest odpowiednia, zalecono wyłącznie w szczególnej sytuacji określonej w art. 11 i 13 jeszcze nieprzyjętej decyzji ramowej o ochronie danych ([18]) i pozostawiono to zadanie państwom członkowskim.

43. W obecnie omawianym przypadku próba obejmuje także cele związane z egzekwowaniem prawa, a rozmowy prowadzi Komisja pod nadzorem Rady. Kontekst sytuacyjny jest inny niż wtedy, gdy oceniano zasady dotyczące bezpiecznego transferu danych osobowych (*safe harbour principles*) lub prawodawstwo kanadyjskie, i bardziej wiąże się z niedawnymi negocjacjami w sprawie danych o przelocie pasażera prowadzonymi z USA i z Australią na mocy prawodawstwa z trzeciego filaru. O zasadach zaproponowanych przez grupę kontaktową wspomniano jednak także w kontekście programu znoszenia wiz, który dotyczy granic i imigracji, a więc kwestii z pierwszego filaru.

44. Inspektor zaleca, aby sprawdzając na mocy przyszłego aktu, czy stopień ochrony danych jest odpowiedni, zawsze korzystano z doświadczeń zebranych we wspomnianych dziedzinach. Zaleca, by w kontekście przyszłego

([16]) Zob. przypis 2.

([17]) Decyzje Komisji o odpowiedniej ochronie danych osobowych w krajach trzecich, m.in. w Argentynie, Kanadzie, Szwajcarii, Stanach Zjednoczonych, na Guernsey, na Wyspie Man i na Jersey, są dostępne pod adresem: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

([18]) Sytuacja ta ogranicza się do przekazywania przez państwo członkowskie krajom trzecim lub instytucjom międzynarodowym danych uzyskanych od właściwego organu innego państwa członkowskiego.

aktu rozwinąć pojęcie „odpowiedniego stopnia ochrony danych", opierając się na podobnych kryteriach jak te, które stosowano we wcześniejszych próbach adekwatności.

Wzajemne uznawanie swoich systemów – reguła wzajemności

45. Drugi element, który składa się na stopień ochrony danych, wiąże się ze wzajemnym uznawaniem przez UE i USA swoich systemów. W tej kwestii sprawozdanie grupy kontaktowej stwierdza, że należy „doprowadzić do wzajemnego uznawania skuteczności systemów ochrony prywatności i danych w dziedzinach objętych przedmiotowymi zasadami" ([19]) oraz do „równorzędnego i wzajemnego stosowania prawa o ochronie prywatności i danych osobowych".

46. Inspektor uważa za oczywiste, że wzajemnie uznawać swoje systemy (reguła wzajemności) można tylko wtedy, gdy gwarantowany jest odpowiedni stopień ochrony danych. Innymi słowy, w przyszłym akcie należy zapewnić zharmonizowany minimalny stopień ochrony (dzięki badaniu stopnia ochrony danych i uwzględnianiu zapotrzebowania na umowy szczegółowe w pojedynczych przypadkach). Tylko pod tym warunkiem może obowiązywać reguła wzajemności.

47. Pierwszym elementem, który należy mieć na uwadze, jest wzajemność merytorycznych przepisów o ochronie danych. Zdaniem Inspektora umowa zrealizuje koncepcję wzajemności merytorycznych przepisów o ochronie danych, o ile zagwarantuje z jednej strony, że przetwarzanie danych na terytorium UE (i USA) będzie się odbywać z pełnym poszanowaniem wewnętrznego prawa o ochronie danych, a z drugiej strony – że przetwarzanie danych objętych przedmiotową umową poza krajem, z którego pochodzą, będzie się odbywać z poszanowaniem przewidzianych w tej umowie zasad ochrony danych.

48. Drugim elementem wzajemności są mechanizmy odwoławcze. Należy dopilnować, by obywatele UE dysponowali odpowiednimi środkami odwoławczymi, gdy dane ich dotyczące będą przetwarzane w USA (niezależnie od tego, na mocy jakiego prawa odbywa się przetwarzanie), ale również – by Unia Europejska i jej państwa członkowskie dawały takie same prawa obywatelom USA.

49. Trzecim elementem jest wzajemność dostępu, jaki do danych osobowych mają organy ochrony porządku publicznego. Jeżeli jakikolwiek akt daje władzom USA dostęp do danych pochodzących z Unii Europejskiej, wzajemność wymaga, by taki sam dostęp do danych pochodzących z USA uzyskały władze UE. Wzajemność nie może osłabić ochrony osoby, której dotyczą dane. To warunek, od którego zależy transatlantycki dostęp organów ochrony porządku publicznego do danych osobowych. Konkretnie oznacza to, że:

— nie należy umożliwiać władzom USA bezpośredniego dostępu do danych znajdujących się na terytorium UE (i odwrotnie). Należy udzielić wyłącznie pośredniego dostępu – na zasadzie przesyłania danych,

— dostęp taki należy zapewnić pod kontrolą organów ochrony danych i władz sądowniczych kraju, w którym odbywa się przetwarzanie danych,

— dostęp władz USA do baz danych w UE powinien się odbywać z poszanowaniem merytorycznych przepisów o ochronie danych (patrz wyżej), a osoba, której dane dotyczą, powinna dysponować pełnymi środkami odwoławczymi.

Precyzja aktu

50. Należy wyszczególnić warunki oceny (odpowiedni stopień ochrony, równoważność, wzajemne uznawanie swoich systemów), ponieważ od tego zależy treść umowy, to znaczy jej precyzyjność, pewność prawa i skuteczność ochrony danych. Treść przyszłego aktu musi być precyzyjna i ścisła.

51. Poza tym należy pamiętać, że każda umowa szczegółowa zawarta w dalszej kolejności będzie musiała przewidywać dokładne i kompletne zabezpieczenia w zakresie ochrony danych w stosunku do osoby, której dotyczą wymieniane dane. Tylko takie dwustopniowe, konkretne zasady ochrony danych sprawią, że umowa ogólna i umowy szczegółowe będą się dopełniać, o czym już wspomniano w pkt 35 i 36 niniejszej opinii.

Wzór dla umów z innymi krajami trzecimi

52. Na szczególną uwagę zasługuje to, do jakiego stopnia umowa z USA może posłużyć za wzór dla umów z innymi krajami trzecimi. Inspektor zwraca uwagę, że w wyżej wspomnianym sprawozdaniu grupy kontaktowej jako strategicznego partnera UE wskazano oprócz USA także Rosję. O ile zasady zawarte w umowie będą neutralne i zgodne z podstawowymi unijnymi zabezpieczeniami, mogą stanowić użyteczny precedens. Jednak przeciw bezpośredniej transpozycji umowy przemawia jej specyfika związana np. z przepisami prawnymi kraju

([19]) Rozdział A. Wiążąca umowa międzynarodowa, s. 8.

otrzymującego dane lub z celem przekazywania tych danych. Równie decydujący będzie stan demokracji w krajach trzecich: należy się upewnić, czy kraj otrzymujący dane będzie faktycznie respektował i skutecznie wdrażał uzgodnione zasady.

Punkty odniesienia pozwalające ocenić stopień ochrony danych

53. Odpowiedni stopień ochrony danych – ewidentny lub domniemany – zawsze powinien być zgodny z międzynarodowymi i europejskimi przepisami prawnymi, a zwłaszcza ze wspólnie uzgodnionymi zabezpieczeniami w dziedzinie ochrony danych. Są one zapisane w wytycznych ONZ, w konwencji Rady Europy nr 108 i protokole dodatkowym do tej konwencji, w wytycznych OECD, w projekcie decyzji ramowej o ochronie danych, a także – w przypadku pierwszego filaru – w dyrektywie 95/46/WE ([20]). We wszystkich tych aktach zamieszczono podobne zasady, które są powszechnie uznawane za podstawę ochrony danych osobowych.

54. To, by wspomniane wyżej zasady zostały należycie uwzględnione, jest tym ważniejsze, jeśli wziąć pod uwagę skutki ewentualnej umowy przedstawione w sprawozdaniu grupy kontaktowej. Akt dotyczący całego sektora *egzekwowania prawa* w kraju trzecim byłby faktycznie sytuacją bez precedensu. Dotychczasowe decyzje o odpowiednim stopniu ochrony danych podlegające pierwszemu filarowi oraz umowy zawarte z krajami trzecimi w ramach trzeciego filaru UE (Europol, Eurojust) zawsze były związane z konkretnym przekazywaniem danych, tymczasem w przedmiotowym przypadku możliwe byłoby przekazywanie danych w dużo szerszym zakresie z uwagi na rozległy cel umowy (zwalczanie przestępstw, bezpieczeństwo krajowe i publiczne, wzmocnienie granic) oraz nieznaną liczbę odnośnych baz danych.

Podstawowe wymogi

55. Warunki, których należy przestrzegać, przekazując dane osobowe do krajów trzecich, zostały przedstawione w dokumencie roboczym Grupy Roboczej Art. 29 ([21]). Wszelkie umowy w sprawie minimalnych zasad dotyczących prywatności powinny przestrzegać tych warunków, a tym samym dbać, by zabezpieczenia w dziedzinie ochrony danych były skuteczne.

— Co do treści: zasady ochrony danych powinny zapewniać wysoki stopień ochrony i spełniać normy zgodne z zasadami UE. 12 zasad zamieszczonych w sprawozdaniu grupy kontaktowej zostanie w tym kontekście dokładnie przeanalizowanych w rozdziale V niniejszej opinii.

— Co do szczegółów: zależnie od charakteru umowy, a zwłaszcza od tego, czy jest ona oficjalną umową międzynarodową, reguły i procedury powinny być wystarczająco szczegółowe, by można było umowę skutecznie wprowadzić w życie.

— Co do nadzoru: aby zadbać o przestrzeganie uzgodnionych reguł, należy ustanowić konkretne mechanizmy kontroli, zarówno wewnętrznej (audyty), jak i zewnętrznej (przeglądy). Mechanizmy te muszą być w równym stopniu dostępne dla obu stron umowy. Nadzór obejmuje mechanizmy służące przestrzeganiu reguł na poziomie ogólnym, np. wspólne mechanizmy przeglądu, oraz na poziomie niższym, np. indywidualne środki odwoławcze.

56. Poza trzema powyższymi podstawowymi wymogami szczególną uwagę należy zwrócić na szczegóły związane z przetwarzaniem danych osobowych w kontekście egzekwowania prawa. Jest to obszar, w którym prawa podstawowe mogą podlegać pewnym ograniczeniom. Należy więc zadbać o zabezpieczenia, które zrekompensują ograniczenie tych praw, zwłaszcza w przypadku poniższych kwestii i ich skutków dla osób fizycznych:

— Przejrzystość: udostępnianie informacji i danych osobowych może w przypadku egzekwowania prawa zostać ograniczone z uwagi na przykład na niejawne dochodzenie. Ponieważ w UE tradycyjnie ustanawia się dodatkowe mechanizmy, by zrekompensować tego typu ograniczenie praw podstawowych (często z udziałem niezależnych organów ochrony danych), należy zadbać, by podobne mechanizmy były dostępne także wtedy, gdy informacje są przekazywane do kraju trzeciego.

— Środki odwoławcze: z powodów wspomnianych powyżej osoby fizyczne powinny mieć możliwość korzystania z alternatywnych sposobów obrony swoich praw, zwłaszcza za pośrednictwem niezależnego organu nadzoru i przed sądem.

— Zatrzymywanie danych: uzasadnienie dla okresu zatrzymywania danych może nie być przejrzyste. Należy dołożyć starań, by nie uniemożliwiało to skutecznego korzystania ze swoich praw przez osoby, których dane dotyczą, lub przez organy nadzoru.

([20]) — Wytyczne ONZ w sprawie skomputeryzowanych rejestrów danych osobowych, przyjęte przez Zgromadzenie Ogólne w dniu 14 grudnia 1990 r., dostępne pod adresem: www.unhchr.ch/html/menu3/b/71.htm
— Konwencja Rady Europy z dnia 28 stycznia 1981 r, o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, dostępna pod adresem: http://www.conventions.coe.int/treaty/en/Treaties/html/108.htm
— Wytyczne OECD w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych, przyjęte w dniu 23 września 1980 r., dostępne pod adresem: http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
— Projekt decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, dostępny pod adresem http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=pl&DosId=193371
— 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, s. 31.

([21]) Dokument roboczy z dnia 24 lipca 1998 r. w sprawie przekazywania danych osobowych do krajów trzecich: stosowanie art. 25 i 26 unijnej dyrektywy o ochronie danych; WP12.

— Odpowiedzialność organów ochrony porządku publicznego: jeżeli nie istnieje prawdziwa przejrzystość, mechanizmy kontrolne, którymi dysponują osoby fizyczne lub instytucje, nie mogą być wszechstronne. Zasadniczą sprawą jest to, by takie kontrole na trwałe ustanowić, mając na uwadze szczególny charakter danych oraz fakt, że na podstawie przetworzonych danych przeciwko osobom fizycznym mogą zostać podjęte środki przymusu. Odpowiedzialność jest kwestią decydującą, jeżeli chodzi o krajowe mechanizmy kontroli w państwie otrzymującym dane, ale także o możliwości przeglądu przysługujące krajowi lub regionowi, z których dane pochodzą. Takie mechanizmy przeglądu przewidziano w umowach szczegółowych, np. w umowie w sprawie danych o przelocie pasażera, i Inspektor zdecydowanie zaleca, by znalazły się także w akcie ogólnym.

V. **ANALIZA ZASAD**

Wprowadzenie

57. W niniejszym rozdziale przeanalizowano 12 zasad zawartych w dokumencie grupy kontaktowej; przyjęto następującą perspektywę:

— Zasady te wskazują, że USA i UE mają co do nich pewne wspólne poglądy, ponieważ można zaobserwować podobieństwa do zasad zawartych w konwencji nr 108.

— Jednak porozumienie co do zasad nie wystarczy. Akt prawny powinien być dostatecznie ścisły, by zapewnić ich przestrzeganie.

— Inspektor ubolewa, że zasadom nie towarzyszy uzasadnienie.

— Przed opracowaniem opisu zasad należy się upewnić, czy obie strony jednakowo rozumieją użyte sformułowania, np. pojęcie danych osobowych lub pojęcie chronionych osób. W związku z tym pożądane byłoby sporządzenie definicji.

1. Szczegółowy cel

58. Pierwsza zasada wymieniona w załączniku do sprawozdania grupy kontaktowej przewiduje, że dane osobowe są przetwarzane do legalnych celów egzekwowania prawa. Jak wspomniano powyżej, dla Unii Europejskiej oznacza to zapobieganie przestępstwom, ich wykrywanie, prowadzenie dochodzeń w ich sprawie lub ich ściganie. Tymczasem w USA egzekwowanie prawa interpretuje się szerzej niż tylko w odniesieniu do przestępstw i rozumie pod tym pojęciem także „wzmacnianie granic oraz cele związane z bezpieczeństwem publicznym i narodowym". Nie jest jasne, jakie mogą być skutki takich rozbieżności. Choć w sprawozdaniu stwierdzono, że w praktyce cele mogą się w dużym stopniu pokrywać, rozstrzygająca będzie dokładna wiedza o tym, do jakiego stopnia się *nie* pokrywają. W sferze egzekwowania prawa, ponieważ podjęte środki mają wpływ na osoby fizyczne, należy ściśle przestrzegać zasady ograniczonego celu, a cele wyraźnie wskazać i opisać. Z uwagi na przewidzianą w sprawozdaniu regułę wzajemności istotne wydaje się także zbliżenie tych celów. Krótko mówiąc, należy sprecyzować, jak rozumiana jest przedmiotowa zasada.

2. Integralność/jakość danych

59. Inspektor z zadowoleniem przyjmuje przepis wymagający dokładności, istotności, terminowości i kompletności danych osobowych jako cech niezbędnych do ich legalnego przetwarzania. Taka zasada jest podstawowym warunkiem wszelkiego skutecznego przetwarzania danych.

3. Niezbędność/proporcjonalność

60. Zasada ta wyraźnie wiąże gromadzone dane z faktem, że są niezbędne do wypełnienia ustanowionych w prawie celów związanych z jego egzekwowaniem. Wymóg istnienia podstawy prawnej to pozytywny element, dający pewność co do legalności przetwarzania danych. Inspektor zwraca jednak uwagę, że choć zasada ta daje większą pewność prawa w przypadku przetwarzania danych, podstawą prawną tego przetwarzania jest ustawodawstwo kraju trzeciego. Ustawodawstwo kraju trzeciego nie może samo w sobie stanowić legalnej podstawy przekazywania danych osobowych ([22]). W kontekście sprawozdania grupy kontaktowej wydaje się, że z zasady uznano legalność ustawodawstwa kraju trzeciego, tzn. USA. Należy pamiętać, że nawet jeśli założenie takie jest uzasadnione w obecnym przypadku, ponieważ USA są państwem demokratycznym, to ten sam schemat nie byłby zasadny w przypadku stosunków z innym krajem trzecim i nie mógłby zostać powielony.

61. Jak stwierdzono w załączniku do sprawozdania grupy kontaktowej, każde przekazanie danych osobowych musi być istotne, niezbędne i odpowiednie. Inspektor podkreśla, że przetwarzanie danych będzie proporcjonalne, gdy nie będzie się wiązać z nadmierną ingerencją, a jego warunki będą wyważone tak, by uwzględnić prawa i interesy osób, których dane dotyczą.

62. Dlatego dostępu do danych należy udzielać na zasadzie pojedynczych przypadków, zależnie od praktycznych potrzeb związanych z konkretnym dochodzeniem. Stały dostęp organów ochrony porządku publicznego z kraju trzeciego do baz danych znajdujących się w UE można by uznać za nieproporcjonalny i niedostatecznie uzasadniony. Inspektor przypomina, że nawet w kontekście obowiązujących umów o wymianie danych, np. umowy w sprawie danych o przelocie pasażera, wymiana

([22]) Zob. zwłaszcza art. 7 lit. c) i e) dyrektywy 95/46/WE. W opinii 6/2002 z dnia 24 października 2002 r. w sprawie przekazywania informacji na temat listy pasażerów i innych danych przez linie lotnicze Stanom Zjednoczonym Grupa Robocza Art. 29 stwierdza, że „nie do zaakceptowania jest, by na podstawie jednostronnej decyzji podjętej przez kraj trzeci z uwagi na jego interes publiczny dochodziło do rutynowego i hurtowego przekazywania danych chronionych przedmiotową dyrektywą".

danych wynika ze szczególnych okoliczności i odbywa się przez ograniczony czas ([23]).

63. Postępując zgodnie z takim samym założeniem, należy uregulować okres zatrzymywania danych: dane należy przechowywać jedynie przez czas potrzebny do wypełnienia realizowanego celu. Jeżeli przestały być istotne dla wskazanego celu, należy je usunąć. Inspektor zdecydowanie sprzeciwia się magazynowaniu danych o osobach niebędących podejrzanymi, na wypadek gdyby dane te okazały się potrzebne w późniejszym czasie.

4. Bezpieczeństwo danych

64. W ramach przedmiotowych zasad przewidziano środki i procedury, które chronią dane przed nadużyciami, modyfikacjami i innymi zagrożeniami, oraz przepisy, które dają dostęp do danych tylko upoważnionym osobom. Inspektor uważa to rozwiązanie za satysfakcjonujące.

65. Dodatkowo można by uzupełnić tę zasadę przepisem o ustanowieniu rejestru osób, które korzystają z dostępu do danych. Zwiększyłoby to skuteczność zabezpieczeń mających ograniczyć dostęp do danych i zapobiec nadużyciom w stosunku do nich.

66. Poza tym należy przewidzieć wzajemne informowanie się o naruszeniu bezpieczeństwa: podmioty z USA i UE otrzymujące dane powinny mieć za zadanie informować partnerów, w razie gdyby dane zostały w sposób bezprawny ujawnione. Przyczyni się to do bardziej odpowiedzialnego przetwarzania danych.

5. Specjalne kategorie danych osobowych

67. Zasadę zabraniającą przetwarzania danych szczególnie chronionych znacznie osłabia – zdaniem Inspektora – odstępstwo pozwalające przetwarzać takie dane, jeśli prawo wewnętrzne przewiduje „odpowiednie zabezpieczenia". Właśnie z uwagi na charakter tych danych wszelkie odstępstwa od zakazu muszą być stosownie i dokładnie uzasadnione i musi im towarzyszyć wykaz celów i okoliczności pozwalających przetwarzać określony rodzaj danych szczególnie chronionych oraz wskazówki co do cech administratorów upoważnionych do przetwarzania tego rodzaju danych. Jeżeli chodzi o zabezpieczenia, które należy wprowadzić, Inspektor uważa między innymi, że dane szczególnie chronione nie powinny same w sobie stanowić powodu do wszczęcia dochodzenia. W pewnych szczególnych okolicznościach mogłyby być udostępniane, ale tylko jako informacje dodatkowe o osobie, wobec której już toczy się dochodzenie. W opisie zasady należy wyliczyć pewną ograniczoną liczbę takich zabezpieczeń i warunków.

6. Odpowiedzialność

68. Jak stwierdzono już w pkt 55–56 niniejszej opinii, należy skutecznie zadbać o odpowiedzialność podmiotów publicznych przetwarzających dane osobowe, a w umowie przewidzieć sposoby egzekwowania takiej odpowiedzialności. Jest to tym ważniejsze, że w kontekście egzekwowania prawa brak jest przejrzystości tradycyjnie związanej z przetwarzaniem danych osobowych. W związku z tym stwierdzenie – zawarte w załączniku do sprawozdania – o odpowiedzialności podmiotów publicznych bez dokładniejszego objaśnienia warunków i skutków takiej odpowiedzialności nie stanowi satysfakcjonującej gwarancji. Inspektor zaleca, by w tekście aktu zamieścić takie objaśnienie.

7. Niezależny i skuteczny nadzór

69. Inspektor w pełni popiera przepis o niezależnym i skutecznym nadzorze ze strony co najmniej jednego publicznego organu nadzoru. Uważa, że należy sprecyzować, jak rozumiana jest taka niezależność, a zwłaszcza od kogo organy te są niezależne i komu podlegają. Do tego celu potrzebne są kryteria, które powinny uwzględniać niezależność instytucjonalną i operacyjną od organów wykonawczych i ustawodawczych. Inspektor przypomina, że to jeden z istotnych elementów, od których zależy, czy można będzie skutecznie egzekwować przestrzeganie zasad. Z uwagi na kwestię odpowiedzialności podmiotów publicznych przetwarzających dane osobowe – o czym mowa wyżej – bardzo istotne jest także, by organom tym przysługiwała możliwość interwencji i egzekwowania prawa. O istnieniu i kompetencjach takich organów należy wyraźnie poinformować osoby, których dane dotyczą, tak by mogły korzystać ze swoich praw, zwłaszcza gdy zależnie od kontekstu przetwarzania danych właściwość przypada kilku organom.

70. Ponadto Inspektor zaleca, by w przyszłej umowie zadbano także o mechanizmy współpracy między organami nadzoru.

8. Indywidualny dostęp do danych i możliwość ich poprawiania

71. Potrzeba szczególnych gwarancji, jeżeli chodzi o dostęp do danych i ich poprawianie w kontekście egzekwowania prawa. W związku z tym Inspektor z zadowoleniem przyjmuje zasadę stwierdzającą, że osobom fizycznym powinien przysługiwać dostęp do ich danych osobowych oraz „możliwość ich poprawiania lub usuwania". Pozostają jednak pewne niejasności co do definicji osób fizycznych (chronione powinny być wszystkie osoby, których dotyczą dane, a nie tylko obywatele danego kraju) i co do sytuacji, w których osoby fizyczne mogłyby się sprzeciwić przetwarzaniu swoich danych. Trzeba sprecyzować, czym są „odpowiednie przypadki", w których można wnieść sprzeciw lub nie można tego zrobić. Dla osób, których dotyczą dane, powinno być jasne, w jakich okolicznościach – np. w zależności

([23]) Umowa wygaśnie i przestanie obowiązywać siedem lat po dniu podpisania, o ile strony wzajemnie nie uzgodnią jej zastąpienia.

od rodzaju organu, rodzaju dochodzenia lub innych kryteriów – będą mogły korzystać ze swoich praw.

72. Poza tym, jeżeli z uzasadnionych powodów nie istnieje bezpośrednia możliwość sprzeciwienia się przetwarzaniu danych, możliwa powinna być pośrednia weryfikacja z pomocą niezależnego organu odpowiedzialnego za nadzór nad przetwarzaniem danych.

9. Przejrzystość i powiadomienia

73. Inspektor jeszcze raz podkreśla, jak ważna jest faktyczna przejrzystość, by umożliwić osobom fizycznym korzystanie ze swoich praw i przyczynić się do ogólnej odpowiedzialności władz publicznych za przetwarzanie danych osobowych. Popiera opracowane zasady i wyraźnie zwraca uwagę, że do obywateli należy kierować zarówno powiadomienia ogólne, jak i indywidualne. Odzwierciedlono to w zasadzie zapisanej w pkt 9 załącznika.

74. Jednak w rozdziale 2 A.B sprawozdania („Uzgodnione zasady") wspomniano, że w USA przejrzystość może obejmować „pojedynczo lub łącznie – publikację w Rejestrze Federalnym, powiadomienie indywidualne oraz upublicznienie w ramach postępowania sądowego". Należy wyjaśnić, że publikacja w dzienniku urzędowym nie jest wystarczającą gwarancją, że osoby, których dotyczą dane, uzyskają odpowiednie informacje. Inspektor przypomina, że potrzeba indywidualnych powiadomień i że informacje należy przedstawić w formie i języku łatwo zrozumiałym dla osób, których dotyczą dane.

10. Środki odwoławcze

75. Aby osoby fizyczne mogły skutecznie korzystać ze swoich praw, muszą mieć możliwość zgłaszania skarg do niezależnego organu ochrony danych oraz możliwość odwoływania się do niezależnego i bezstronnego sądu. Obie te możliwości powinny być równie dostępne.

76. Dostęp do niezależnego organu ochrony danych jest niezbędny, ponieważ zapewnia elastyczną i mniej kosztowną pomoc w kontekście egzekwowania prawa, który dla obywateli może być dość nieprzejrzysty. Organy ochrony danych mogą także świadczyć pomoc, korzystając – w imieniu osób, których dotyczą dane – z prawa dostępu do ich danych, jeżeli wyjątkowe okoliczności uniemożliwiają tym osobom bezpośredni dostęp do tych danych.

77. Dostęp do sytemu sądowego jest dodatkową i nieodzowną gwarancją tego, że osoby, których dane dotyczą, będą mogły się odwołać do organu reprezentującego w systemie demokratycznym inny rodzaj władzy niż instytucje publiczne przetwarzające dane tych osób. Taki skuteczny środek pozwalający odwołać się do sądu został uznany przez Europejski Trybunał Sprawiedliwości ([24]) za „niezbędny, by zapewnić obywatelom skuteczną ochronę ich praw. (…) Odzwierciedla on ogólną zasadę prawa wspólnotowego, która podkreśla tradycje konstytucyjne wspólne państwom członkowskim i została zapisana w art. 6 i 13 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności". Istnienie sądowego środka odwoławczego wyraźnie przewidziano w art. 47 Karty praw podstawowych Unii Europejskiej oraz w art. 22 dyrektywy WE 95/46 – niezależnie od wszelkich administracyjnych środków odwoławczych.

11. Zautomatyzowane decyzje w indywidualnych sprawach

78. Inspektor z zadowoleniem przyjmuje przepis przewidujący odpowiednie zabezpieczenia w przypadku automatycznego przetwarzania danych osobowych. Zwraca uwagę, że warunki stosowania tej zasady stałyby się jaśniejsze, gdyby wspólnie ustalono, co oznaczają „znaczące niekorzystne działania dotyczące stosownych interesów osoby fizycznej".

12. Przekazywanie danych kolejnym krajom

79. Niektóre z warunków decydujących o przekazaniu danych kolejnym krajom są niejasne. Przede wszystkim należy sprecyzować tam, gdzie jest mowa o tym, że przekazywanie danych kolejnym krajom musi być zgodne z międzynarodowymi ustaleniami i umowami między krajem wysyłającym dane a krajem je odbierającym, czy zapis ten odnosi się do dwóch krajów, które zapoczątkowały pierwsze przekazanie danych, czy do dwóch krajów, między którymi odbywa się dalsze przekazanie. Inspektor jest zdania, że umowy pomiędzy dwoma krajami, które zapoczątkowały pierwsze przekazanie danych, są potrzebne w każdym przypadku.

80. Inspektor zwraca również uwagę na bardzo szeroką definicję „legalnego interesu publicznego", który jest podstawą przekazania danych dalszym krajom. Zakres bezpieczeństwa publicznego pozostaje niejasny, a objęcie przekazywaniem danych także przypadków naruszenia etyki zawodów regulowanych wydaje się w kontekście egzekwowania prawa nieuzasadnione i nadmierne.

VI. **WNIOSKI**

81. Inspektor z zadowoleniem przyjmuje wspólne prace władz UE i USA w dziedzinie egzekwowania prawa, dla której ochrona danych jest sprawą kluczową. Chciałby mimo to wyraźnie zwrócić uwagę na fakt, że problem jest złożony – zwłaszcza jeśli chodzi o jego dokładny zakres i charakter – a zatem wymaga uważnej i wnikliwej analizy. Należy

([24]) Sprawa 222/84, *Johnston* Zb. Orz. 1986, s. 1651; sprawa 222/86, *Heylens* Zb. Orz. 1987, s. 4097; sprawa C-97/91 *Borelli* Zb. Orz. 1992, s. I-6313.

uważnie przeanalizować wpływ transatlantyckiego aktu na ochronę danych, biorąc przy tym pod uwagę obowiązujące przepisy prawne i skutki dla obywateli.

82. Inspektor apeluje o większą precyzję i uszczegółowienie postanowień zwłaszcza w następujących sprawach:

— Określenie charakteru aktu, który – by gwarantować dostateczną pewność prawa – powinien być prawnie wiążący;

— Dokładne badanie odpowiedniego stopnia ochrony danych, oparte na zasadniczych wymogach odnoszących się do treści, szczegółów i nadzoru systemu. Inspektor uważa, że aktem ogólnym można zapewnić odpowiedni stopień ochrony danych tylko wtedy, gdy aktowi temu będą towarzyszyć odpowiednie umowy szczegółowe zawierane w pojedynczych przypadkach;

— Wyraźnie wskazany zakres zastosowania umowy oraz jasne wspólne definicje przedmiotowych celów związanych z egzekwowaniem prawa;

— Precyzyjne warunki, na których w systemie przekazywania danych mogą uczestniczyć podmioty prywatne;

— Przestrzeganie zasady proporcjonalności, tzn. dokonywanie wymiany danych w pojedynczych przypadkach, gdy zaistnieje konkretna potrzeba;

— Silne mechanizmy nadzoru oraz mechanizmy odwoławcze dostępne osobom, których dotyczą dane, w tym administracyjne i sądowe środki odwoławcze;

— Skuteczne środki gwarantujące osobom, których dotyczą dane, niezależnie od obywatelstwa, możliwość korzystania ze swoich praw;

— Zaangażowanie niezależnych organów ochrony danych zwłaszcza w nadzór i w pomoc osobom, których dotyczą dane.

83. Inspektor wyraźnie zwraca uwagę na fakt, że opracowując przedmiotowe zasady, należy unikać pośpiechu, który prowadziłby w przypadku ochrony danych do niesatysfakcjonujących rozwiązań powodujących skutki odwrotne do zamierzonych. Najlepszym rozwiązaniem w obecnej chwili byłoby przygotowanie planu prac, który prowadziłby do ewentualnego sporządzenia umowy na późniejszym etapie.

84. Inspektor apeluje również o większą przejrzystość podczas opracowywania zasad rządzących ochroną danych. Tylko dzięki zaangażowaniu wszystkich zainteresowanych stron, w tym Parlamentu Europejskiego, przyszły akt odniesie korzyść z demokratycznej debaty i zdobędzie niezbędne poparcie i uznanie.

Sporządzono w Brukseli, dnia 11 listopada 2008 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych