

SYSTEM INFORMACJI WIZOWEJ (VIS) I WYMIANA INFORMACJI POMIĘDZY PAŃSTWAMI CZŁONKOWSKIMI W PRZEDMIOCIE WIZ JEDNOLITYCH KRÓTKOTERMINOWYCH

ARTUR MODRZEJEWSKI

University of Białystok, Faculty of Law, Poland

Abstract in original language:

Celem niniejszej publikacji będzie przybliżenie zasady funkcjonowania systemu VIS, a także analiza problemów jakie wiążą się z jego działaniem. Szczególna uwaga poświęcona zostanie problematyce wymiany danych osobowych pomiędzy państwami członkowskimi i określeniu zasad dostępu do systemu i umieszczonych w nim informacji.

Key words in original language:

System Informacji Wizowej (VIS), wiza jednolite krótkoterminowe, wymiana danych.

Abstract:

The purpose of this article is to present problem, how to ensure the need for using the data processing records in order to ensure the security of data, and details the respective responsibilities to ensure this security level.

Key words:

Visa Information System (VIS), short stay visa, data exchange.

1. UTWORZENIE SYSTEMU INFORMACJI WIZOWEJ

Obok SIS (Systemu Informatycznego Schengen) i EURODAC, System Informacji Wizowej (VIS) jest trzecią największą platformą informatyczną mającą służyć do przechowywania i wymiany danych osobowych. VIS ma magazynować dane osób starających się o wydanie wiz, by następnie dane te mogły być konsultowane i sprawdzane przez organy odpowiedzialne za ochronę granic zewnętrznych Unii Europejskiej.

Utworzenie Systemu Informacji Wizowej (VIS) stanowi ważną część wspólnej polityki wizowej UE i jest objęte wieloma powiązаныmi instrumentami. W kwietniu 2003 r. na zlecenie Komisji zostało opracowane studium wykonalności w odniesieniu do VIS¹. We wrześniu 2003 r. Komisja zaproponowała wprowadzenie zmiany do poprzedniego rozporządzenia ustalającego jednolity format wiz². Zasadniczym celem było wprowadzenie do nowego formatu wiza danych biometrycznych (zdjęcie twarzy i dwa odciski palców). Dane biometryczne miałyby być przechowywane w mikrochipie. W czerwcu 2004 r. decyzją Rady został rozpoczęty proces tworzenia Systemu Informacji Wizowej poprzez zapewnienie podstawy prawnej do włączenia do budżetu UE środków na rozwój VIS³. W decyzji tej

¹ System Informacji Wizowej, sprawozdanie w wersji ostatecznej, zlecone przez WE i przeprowadzone przez Trasyk w kwietniu 2003 r.

²COM(2003)558 wersja ostateczna oraz 2003/0217 (CNS) i 2003/0218 (CNS).

³ Dz.U. L 213, z 15.06.2004, 2004/512/WE, s. 5.

zaproponowano utworzenie centralnej bazy danych złożonej z informacji związanych z wnioskami o wydanie wiz i uruchomienie procedury "komitologii"⁴ w celu opracowania rozwiązań technicznych stosowanych do VIS. W grudniu 2004 r. Komisja przyjęła wniosek dotyczący rozporządzenia w sprawie VIS oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych⁵. Jednakże jednocześnie podkreśla się, że dla prawidłowego działania VIS konieczne będzie przedsięwzięcie dalszych instrumentów prawnych, w tym:

- A) Poprawienie Wspólnych Instrukcji Konsularnych w sprawie wiz dla misji dyplomatycznych i urzędów konsularnych Stron Umawiających się do Konwencji z Schengen, związane z obowiązkową rejestracją danych biometrycznych, łącznie z określeniem przypadków, w których nastąpi zwolnienie z tego obowiązku;
- B) Opracowanie nowych mechanizmów wymiany danych z Irlandią i Zjednoczonym Królestwem;
- C) Wymiana danych dotyczących wiz długoterminowych, ze szczególnym uwzględnieniem wiz długoterminowych, które nie są równocześnie ważne jako wizy krótkoterminowe.⁶

Zgodnie z decyzją podjętą przez Radę ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych w skład VIS będą wchodziły dwie bazy danych, gdzie kumulowane będą wnioski o wydanie wizy: Centralny System Informacji Wizowej (CS-VIS) i Krajowy Interfejs (NI-VIS) znajdujący się w państwach Schengen. Obowiązkiem państw Schengen będzie wyznaczenie krajowego organu centralnego połączonego z Krajowym Interfejsem, za pośrednictwem, którego właściwe organy będą mieć dostęp do CS-VIS⁷.

Wciąż toczą się prace nad regulacjami prawnymi, dającymi podstawy legislacyjne do podejmowania działań faktycznych. Do nowszych aktów należą decyzja Komisji z dn. 22.09.2006 r. ustanawiająca specyfikacje techniczne dotyczące norm przyjętych dla cech

⁴ „komitologia”- współpraca komitetów powołanych przez Radę Unii Europejskiej z Komisją Europejską nad wdrażaniem postanowień Rady Unii Europejskiej. Traktat o Europejskiej Wspólnocie Gospodarczej na mocy artykułu 145 powierza Komisji Europejskiej kompetencje wykonawcze do uchwalonych przez Radę aktów prawnych. Rada monitoruje działania wykonawcze Komisji poprzez ustanowione komisje doradcze, zarządzające oraz regulujące, które składają się z ekspertów narodowych. Komisje doradcze mają tylko możliwość wydawania niewiążących zaleceń Komisji Europejskiej. Komisje zarządzające mogą się zwrócić do Rady UE o zbadanie środków wykonawczych zastosowanych przez Komisję w określonym terminie, podczas którego procedura wdrażania jest zawieszona. Jeśli Rada nie podejmie w tym terminie decyzji, Komisja może kontynuować proces wykonawczy. Komisje regulujące mają również prawo zawieszenia działań wykonawczych Komisji i zwrócenia się do Rady UE w celu zbadania środków wykonawczych. Jeśli Rada w określonym terminie nie podejmie decyzji Komisja może kontynuować proces wykonawczy tylko, jeśli Rada nie odrzuciła prostą większością głosów środków wykonawczych. Komitologia daje Radzie UE kontrolę nad władzą wykonawczą pozostającą w rękach Komisji Europejskiej.

⁵ Bruksela dn. 28.12.2004r., COM(2005)835 końcowy, 2004/0287 (COD).

⁶ Tamże, s.3.

⁷ Decyzja Rady z dn.08.06.2004r. w sprawie Ustanowienia Wizowego Systemu Informacyjnego VIS, (2004/512/WE), art.1 i 2.

biometrycznych na potrzeby rozwoju Wizowego Systemu Informacyjnego⁸, decyzja ta określa normy techniczne, które umożliwią sprostanie wymogom jakości i wiarygodności identyfikatorów biometrycznych. Istotna jest również decyzja Komisji z dn. 03.11.2006 r. ustanawiająca lokalizację Wizowego Systemu Informacyjnego (VIS) w fazie jego rozwoju.⁹ W fazie rozwoju centralna jednostka VIS będzie zlokalizowana w Strasburgu (Francja), zaś centralna jednostka rezerwowa zlokalizowana będzie w Sankt Johann w Pongau (Austria).¹⁰

Celem niniejszej publikacji będzie przybliżenie zasady funkcjonowania systemu VIS, a także analiza problemów jakie wiążą się z jego działaniem. Szczególna uwaga poświęcona zostanie problematyce wymiany danych osobowych pomiędzy państwami członkowskimi i określeniem zasad dostępu do systemu i umieszczonych w nim informacji.

2. CEL FUNKCJONOWANIA VIS

Rozwój wspólnej polityki wizowej wymaga skutecznej wymiany odpowiednich danych. VIS jest jednym z mechanizmów, który może zapewnić niezakłócony przepływ informacji. Jednakże ten nowy instrument powinien ograniczać się do gromadzenia i wymiany danych, pod warunkiem, że gromadzenie i ich wymiana są konieczne do rozwoju wspólnej polityki wizowej. Ograniczony cel systemu odgrywa zasadniczą rolę w określaniu właściwej zawartości i wykorzystania systemu zgodnie z prawem, a zatem również w udzielaniu prawa dostępu do VIS organom państw Schengen dla ochrony interesu publicznego.¹¹

Cel VIS ma olbrzymie znaczenie, zarówno w świetle art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka, jak i w szerszym kontekście ochrony danych osobowych. Zgodnie z art. 6 dyrektywy 95/46/WE dane osobowe muszą być "gromadzone do określonych, wyraźnych i legalnych celów oraz nie będą poddawane dalszemu przetwarzaniu w sposób niezgodny z tymi celami"¹². Tylko precyzyjne określenie celów, jakie VIS ma realizować, pozwoli na właściwą ocenę proporcjonalności i adekwatności przetwarzania danych osobowych, która jest niezwykle istotna z powodu charakteru danych, skali operacji przetwarzania, ochrony praw cudzoziemców, których dane dotyczą.

Cel VIS jest określony w art. 2 rozporządzenia: Celem VIS jest poprawa realizacji wspólnej polityki wizowej, poprawa współpracy konsularnej i procesu konsultacji pomiędzy

⁸ Decyzja Komisji z dn. 22.09.2006 r. ustanawiająca specyfikacje techniczne dotyczące norm przyjętych dla cech biometrycznych na potrzeby rozwoju Wizowego Systemu Informacyjnego (2006/648/WE).

⁹ Decyzja Komisji z dn. 03.11.2006 r. ustanawiająca lokalizację Wizowego Systemu Informacyjnego (VIS) w fazie jego rozwoju Nr C(2006) 5161.

¹⁰ Europejski Inspektor Ochrony Danych: Opinia w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych (COM(2004)835 wersja ostateczna).

¹¹ Europejski Inspektor Ochrony Danych: Opinia w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie... (COM(2004)835 wersja ostateczna,

¹² Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dn.24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, DZ. U. W. E. L 281/31.

centralnymi organami wizowymi poprzez ułatwienie wymiany danych pomiędzy państwami członkowskimi o wnioskach i związanych z nimi decyzjach.¹³ Zatem wszystkie elementy składające się na VIS muszą być koniecznymi i proporcjonalnymi instrumentami służącymi osiągnięciu tego celu.

Ideą przewodnią konstruowania systemu VIS było usprawnienie realizacji wspólnej polityki wizowej. Art. 2 rozporządzenia w sprawie VIS przedstawia wykaz dodatkowych korzyści płynących z usprawnienia polityki wizowej, takich jak:

- A) uproszczenia procedury składania wniosków wizowych;
- B) zapobieżenia omijaniu kryteriów służących do określania, które państwo członkowskie odpowiada za rozpatrzenie wniosku;
- C) ułatwienia walki z nadużyciami;
- D) ułatwienia odpraw w przejściach granicznych na granicach zewnętrznych państw członkowskich i na terytorium państw członkowskich;
- E) pomocy w identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium państw członkowskich lub też przestały spełniać te warunki;
- F) ułatwienia stosowania rozporządzenia (WE) nr 343/2003;
- G) przyczynienia się do zapobiegania zagrożeniom bezpieczeństwa
- H) wewnętrznego każdego z państw członkowskich¹⁴

Wskazane zadania, dla których realizacji powołany został system VIS, stanowią jednocześnie pozytywne przykłady jego funkcjonowania.

Głównym celem funkcjonowania VIS jest więc usprawnienie wspólnej polityki wizowej, poprzez ułatwienie wymiany danych pomiędzy państwami Schengen dzięki utworzonej centralnej bazie danych. Istotnym elementem funkcjonowania systemu jest wprowadzanie danych biometrycznych (fotografia i odcisk palca) do procedury składania wniosków oraz przechowywanie tych danych w centralnej bazie danych. Dane biometryczne mogą być również wykorzystywane na naklejce wizowej.¹⁵

¹³ Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz. Urz. UE L 218.

¹⁴ Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS)

¹⁵ Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS)

Jednocześnie nie można przeceniać celu, dla którego VIS powstaje. Podstawowym jego zadaniem jest ograniczenie handlu wizami i rozpowszechnianiu się oszustw wizowych, jak również wzmocnienie współpracy konsularnej. Ochrona bezpieczeństwa i porządku publicznego będzie realnie realizowana jedynie w niewielkim stopniu. Choćby, dlatego że w systemie, jako jednostki niebezpieczne będą zarejestrowani tylko ci cudzoziemcy, którzy już w przeszłości w sposób legalny dostali się na terytorium Unii i tam popełnili czy niedozwolony, zagrażający bezpieczeństwu powszechnemu. W odniesieniu do powyższego warto również zauważyć, że "Wytyczne do wprowadzenia wspólnego systemu wymiany danych wizowych" przyjęte przez Radę ds. WSiSW w dniu 13 czerwca 2002 r. umieszczają zapobieganie zagrożeniom dla bezpieczeństwa wewnętrznego na końcu listy¹⁶. Co określa miejsce „zapewnienia bezpieczeństwa wewnętrznego” w hierarchii celów realizowanych przez VIS.

W rozszerzonej ocenie wpływu zostaje jednoznacznie stwierdzone, że: „brak skuteczności w zwalczaniu handlu wizami, oszustw i w przeprowadzaniu odpraw pociąga za sobą również brak skuteczności w odniesieniu do bezpieczeństwa wewnętrznego Państw Schengen”.¹⁷ To oznacza, że zagrożenia dla bezpieczeństwa częściowo wynikają z nieskutecznej polityki wizowej. Pierwszą rzeczą do zrobienia w tej sprawie jest usprawnienie polityki wizowej, głównie poprzez zwalczanie oszustw i skuteczniejsze przeprowadzanie odpraw. Poprawa stanu bezpieczeństwa będzie wynikiem usprawnienia polityki wizowej. W oparciu o te przesłanki należy skoncentrować się na następujących kwestiach:

- A) Proporcjonalności i adekwatności danych i ich wykorzystywaniu (np. kategorie danych, dostęp do danych dla zainteresowanych organów, okres przechowywania);
- B) Korzystaniu z systemu (np. zakres odpowiedzialności i bezpieczeństwo);
- C) Prawie osób, których dane dotyczą (np. informacje, możliwość zmian lub usunięcia niedokładnych lub nieistotnych danych);
- D) Monitorowaniu i nadzorze nad systemem.

System VIS, zgodnie z Rozporządzeniem VIS, może służyć do celów innych niż tylko rozpatrzenie wniosku wizowego i wydanie decyzji wizowej w sprawie wizen Schengen. Wyszukanie danych cudzoziemca w systemie centralnym VIS może posłużyć kompetentnym organom także do sprawdzenia autentyczności wizen.

Dla potrzeb dokonania weryfikacji tożsamości cudzoziemca oraz sprawdzenia autentyczności wizen lub w celu sprawdzenia czy spełnione zostały warunki legalnego wjazdu lub pobytu cudzoziemca na terytorium państwa członkowskiego właściwe organy odpowiedzialne za przeprowadzanie kontroli granicznej lub kontroli wewnątrz kraju będą miały dostęp do danych zawartych w Systemie Informacji Wizowej.

¹⁶ Decyzja ramowa Rady z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu (2002/475/WSiSW), Dz.U. L 164 z 22.06.2002, str. 3.

¹⁷ Analiza rozszerzonej oceny wpływu systemu informacji wizowej, sprawozdanie EPEC (European Policy Evaluation Consortium - Europejskie Konsorcjum ds. Oceny Polityki Europejskiej) w wersji ostatecznej grudzień 2004 r., s. 6, §2.7.

System ułatwiał również będzie identyfikację cudzoziemca. Zadaniem systemu będzie również pomoc w wyszukiwaniu danych koniecznych dla rozpatrywania wniosków o nadanie statusu uchodźcy. W tym celu, zgodnie z art. 9 Rozporządzenia (WE) nr 343/20032, właściwe organy będą miały dostęp do danych zawartych w VIS za pośrednictwem „Systemu Pobyt” - komponentu stanowiącego część VIS. W ten sposób organy wewnętrzne będą w stanie sprawdzić, czy w bazie zarejestrowana jest wiza posiadająca datę wygaśnięcia w terminie nie dłuższym niż sześć miesięcy przed datą złożenia wniosku o nadanie statusu uchodźcy, lub wiza o przedłużonym okresie ważności z datą wygaśnięcia w terminie nie dłuższym niż sześć miesięcy przed datą złożenia wniosku o nadanie statusu uchodźcy. VIS ma być również używany do celów sprawozdawczo – statystycznych, jako doskonałe źródło informacji na temat złożonych i rozpatrzonych wniosków wizowych.

Funkcjonowanie VIS ma wpływ na poprawę i zbliżenie standardów w zakresie przeciwdziałania oszustwom wizowym i fałszowaniu dokumentów. VIS stymulował będzie również rozwój współpracy konsularnej i pomiędzy organami krajowymi odpowiedzialnymi za system. Zarówno w obszarze wspólnej realizacji szkoleń z zasad funkcjonowania systemu, jak i konieczności tworzenia jednolitych baz danych i jednolitych systemów informatycznych, tak by wszelkie dane wprowadzane do VIS mogły być bez problemu tam przesyłane a w dalszej konsekwencji weryfikowane.

Państwa członkowskie pozytywnie odnosiły się do samej idei utworzenia systemu VIS. W szczególności, jeśli chodzi o te kraje, które wcześniej miały własne krajowe systemy zawierające dane wizowe. Dla przykładu Szwecja już wcześniej dysponowała krajowym systemem zarządzania wizami o nazwie Wilma, w którym rejestrowało się wszystkie wnioski o wize do Szwecji ze wszystkich szwedzkich konsulatów na świecie. We Włoszech, podobnie jak w Szwecji, istniał krajowy system kontroli wiz, podobnie w Niemczech czy Francji. Konsulaty wszystkich tych państw oczekiwały i oczekują od VIS znacznego ułatwienia w swej pracy związanej z rozpatrywaniem wniosków wizowych.¹⁸

Zastosowanie biometrii w systemach informatycznych nie jest wyborem bez znaczenia, zwłaszcza w sytuacji, w której system obejmuje tak wielką liczbę osób. Biometria¹⁹ to nie tylko jedna z technologii informatycznych. Zmienia ona w sposób nieodwracalny stosunek pomiędzy ciałem a tożsamością. Cechy ciała ludzkiego stają się przedmiotem odczytu maszynowego i mogą być dalej wykorzystywane. Dlatego też tak istotna jest potrzeba wprowadzenia rygorystycznych zabezpieczeń w odniesieniu do wykorzystania danych

¹⁸ H. Lax: *Sprawozdanie delegacji komisji LIBE z wizyty w Algierii*, Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Bruksela, 16. 11.2006r., www.europarl.europa.eu/meetdocs/2004_2009/documents/pv/638/638724/638724pl.pdf.

¹⁹ Biometrią - ogólnie można nazwać badanie i rozwijanie statystycznych i matematycznych metod stosowanych do analizy danych w naukach biologicznych. Nazwa biometria pochodzi od greckich słów *bio-* życie, *metric-* miara. Klasyfikacja metod biometrycznych: 1. Statyczne (fizjologiczne): metoda Bertillona, odciski palców, rozpoznawanie twarzy, skan tęczówki, skan siatkówki, geometria dłoni, dopasowywanie wzorców naczyń krwionośnych. 2. Dynamiczne (behawioralne): rozpoznawanie mowy, rozpoznawanie pisma odręcznego, odstępny między kliknięciami klawiszy klawiatury podczas pisania (Keystrokedynamics). Pomiedzy danymi, które mogą być użyte do celów identyfikacji znajdują się również fotografie. Jednakże przy obecnym poziomie technologii związanej z automatycznym rozpoznawaniem twarzy dla systemów informatycznych o tak dużej skali, fotografie samodzielnie nie mogą być używane do identyfikacji. Nie mogą zapewnić wiarygodnego wyniku. Zatem nie należy traktować ich za dane adekwatne do celów identyfikacyjnych.

biometrycznych oraz dokładnego zastanowienia się i przeprowadzenia dyskusji w trakcie procesu legislacyjnego.

Dane biometryczne gwarantują prawie absolutnie pewne rozróżnienie, tj. każda osoba posiada niepowtarzalne dane biometryczne. Prawie nigdy nie ulegają zmianie na przestrzeni całego życia, co zapewnia trwałość tych cech. Każda osoba posiada takie same "elementy" fizyczne, co nadaje danym biometrycznym wymiar uniwersalny. Równocześnie usunięcie danych biometrycznych jest prawie niemożliwe. Ten pozytywny aspekt, w przypadku kradzieży „tożsamości” stanowić może dużą wadę. Przechowywanie odcisków palców i fotografii w bazie danych, w powiązaniu ze skradzionym dokumentem może prowadzić do poważnych i trwałych problemów dla prawdziwego posiadacza danej tożsamości. Ponadto dane biometryczne ze swojej natury nie stanowią tajemnicy i mogą nawet zostawiać ślady (odciski palców, DNA), które pozwalają na gromadzenie tych danych bez wiedzy ich posiadacza.

Ze względu na opisane ryzyko, jakie niesie za sobą wykorzystywanie danych biometrycznych, należy wprowadzić w życie istotne zabezpieczenia (zwłaszcza w odniesieniu do zasady ograniczonego celu, ograniczeń dostępu i środków bezpieczeństwa). Konstrukcja takiego systemu zawierającego dane biometryczne powoduje konieczność postawienia pytania o granicę ingerencji administracji w sferę indywidualnej ochrony praw jednostki, w szczególności o granicę naruszania jej prywatności. Systemy ewidencyjne można podzielić na te, których główną funkcją jest ewidencjonowanie danych osób niebezpiecznych, czy takie, które zawierają dane osobowe wszystkich identyfikujących się danym dokumentem. Główną funkcją, jaką spełnia np. SIS jest ewidencjonowanie danych osób niebezpiecznych, system ten jest swego rodzaju rejestrem karnym. Chodzi o lepszą identyfikację osób poszukiwanych, gromadzenie danych osobowych w bazach danych zawierających rejestr karny jest uzasadnione ze względu na przeszłe i rzeczywiste bądź podejrzewane zachowanie jednostki. Jednak w przypadku EURODAC lub VIS sytuacja jest inna. Ubieganie się o azyl, ani złożenie wniosku wizowego, w żaden sposób nie wskazuje na to, że osoba dotychczas niewinna popełni przestępstwo lub akt terrorystyczny. Dlatego też zasada proporcjonalności wymaga, by bazy te konsultowane były wyłącznie dla celów zapobiegania poważnym przestępstwom karnym lub terrorystycznym, prowadzenia śledztw w takich sprawach lub identyfikacji osoby podejrzewanej o popełnienie przestępstwa lub czynu terrorystycznego. Dlatego też próg wymagań, które organy odpowiedzialne za bezpieczeństwo wewnętrzne muszą spełnić, by uzyskać dostęp do EURODAC, VIS, musi być zawsze znacznie wyższy niż próg wymagań w przypadku konsultacji baz danych zawierających rejestr karny²⁰. Dlatego, aby zapewnić pełne przestrzeganie praw określonych w Karcie Praw Podstawowych Unii Europejskiej, zakres dostępu powinien być ograniczony do określonego rodzaju czynów, np. przestępstw terrorystycznych²¹, oraz przestępstw wchodzących w zakres kompetencji Europolu.

Wprowadzenia danych biometrycznych we wcześniejszym etapie było konsultowane z konsulami poszczególnych państw członkowskich. Urzędnicy konsulatów wyrażali dość otwarte stanowisko. Biometria uważana jest za użyteczną, zwłaszcza w przypadku odmiennych alfabetów, gdy identyfikacja nazwiska danej osoby jest bardzo trudna, lub w

²⁰ A. Modrzejewski: *Dokumenty tożsamości i systemy ewidencji ludności – rozwiązania polskie na tle rozwiązań unijnych*, „Wspólnoty Europejskie” nr 5 (192) 2008, s. 30.

²¹ Decyzja ramowa Rady 2002/475/WSiSW

krajach takich jak latynoamerykańskie, w których osoby posiadają różne nazwiska ze względu na podwójne obywatelstwo. Jednocześnie jednak znaleźć można głosy, że w przypadku, gdy wymaga się od obywateli państw trzecich, aby poddali się identyfikacji biometrycznej, należałoby zaoferować im coś w zamian, np. uproszczenie procedury lub krótszy czas oczekiwania.²²

Dane biometryczne są czymś ponadnarodowym, interpretacja ich nie zależy od państwa członkowskiego, są one obiektywnym czynnikiem identyfikującym cudzoziemca. Ich wprowadzenie do wiz można uznać za pozytywny przejaw działań w kierunku stworzenia jednolitego unijnego systemu wizowego.

3. DOSTĘP DO DANYCH I ICH WYKORZYSTYWANIE

Prawidłowe określenie zasad dostępu do danych i ich wykorzystania ma duże znaczenie ze względu na ochronę interesów praw jednostki. Utworzenie takiego rejestru jak VIS przewidywać należy jedynie wtedy, jeżeli dostęp do niego byłby ściśle ograniczony oraz jeżeli przeszukanie rejestru uzasadnione byłoby nadrzędną i bezwzględną potrzebą zagwarantowania bezpieczeństwa publicznego. Tu z kolei pojawia się problem nie tylko jednolitego określenia katalogu organów posiadających uprawnienie do wglądu do systemu, ale również precyzyjne wskazanie sytuacji, w których można korzystać z zawartych w systemie danych osobowych. Można spotkać opinie Europejskiego Inspektora Ochrony Danych odnoszące się do zasad funkcjonowania jednolitego wzoru dokumentów pobytowych²³, czy Systemu Informacji Wizowej²⁴, w których szczególną uwagę zwraca się właśnie na precyzyjne określenie katalogu organów uprawnionych do wglądu w dane biometryczne, osobowe, posiadaczy tych dokumentów. Zwraca się również uwagę na konieczność ustanowienia jednolitych i precyzyjnych zasad sprawowania kontroli nad tymi organami w zakresie przetwarzania danych.

W przypadku VIS każdy organ ma dostęp do różnych danych do różnych celów. Jest to słuszne podejście. Identyfikacja ma bowiem dwa znaczenia. Po pierwsze "sprawdzenie tożsamości osoby", które oznacza porównanie "indywidualne". Jak również "sprawdzenie autentyczności wizy". Zgodnie ze normami Organizacji Międzynarodowego Lotnictwa Cywilnego (ICAO) mikrochip znajdujący się na wizie może korzystać z

²² H. Lax: *Sprawozdanie delegacji...*(*op. cit.*), s.3.

²³ Opinia Europejskiego Inspektora Ochrony Danych w sprawie zmienionego wniosku dotyczącego rozporządzenia Rady zmieniającego rozporządzenie (WE) nr 1030/2002 ustanawiające jednolity wzór dokumentów pobytowych dla obywateli państw trzecich. 28.12.2006, 2006/C 320/10, Dz. Urz. C 320/21.

²⁴ Europejski Inspektor Ochrony Danych: Opinia w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie Systemu Informacji Wizowej (VIS) oraz wymiany danych pomiędzy Państwami Członkowskimi na temat wiz krótkoterminowych (COM(2004)835 wersja ostateczna)

publicznego/prywatnego "systemu klucza" (PKI — Public Key Infrastructure)²⁵ w celu sprawdzenia autentyczności wizy²⁶.

Dlatego też dostęp do chronionego mikrochipu, a co za tym idzie do danych zawartych w VIS powinny mieć wyłącznie organy właściwe do przeprowadzania kontroli wiz. Pozostaje pytanie o liczbę i kompetencje tych organów. Wykaz organów, posiadających dostęp do VIS, wyznaczonych przez każde Państwo Schengen, ma być corocznie publikowany w Dzienniku Urzędowym Unii Europejskiej.²⁷

Większa liczba organów posiadająca połączenie z VIS, może zwiększać ryzyko nadużyć. Zbytne rozszerzenie zakresu organów uprawnionych do wglądu do systemu mogłoby być również rozwiązaniem droższym, zważywszy, że pociągnie za sobą znaczny wzrost liczby bezpiecznych i kontrolowanych dostępów do VIS oraz zapotrzebowania na szkolenia dotyczące takiego dostępu.

Organy uprawnione posiadające dostęp do systemu określone są za pomocą zakresu przypisanych im zadań. Są to:

- A) Organy właściwe do przeprowadzania kontroli wizowych na granicach zewnętrznych i w obrębie terytorium państwa Schengen,
- B) Właściwe organy imigracyjne,
- C) Właściwe organy zajmujące się sprawami azylu.²⁸

Należy stwierdzić, że definicja dotycząca organów posiadających dostęp (do danych) powinna być dokładniejsza. W szczególności nie jest jasne, jakich organów dotyczy określenie "organy właściwe do przeprowadzania kontroli na terytorium państwa Schengen". Należałoby być może przyjąć, że dotyczy to organów właściwych do przeprowadzania kontroli wiz.

Jednocześnie powstaje pytanie o to, czy dostęp do danych zawartych w systemie powinny mieć organy, które nie są zaangażowane w postępowanie w przedmiocie wydania wizy, a ich zadaniem jest zapewnienie bezpieczeństwa na obszarze państw członkowskich. Chodzi tu o głównie organy ścigania.

²⁵ Infrastruktura Klucza Publicznego- jest to szeroko pojęty kryptosystem, w skład którego wchodzi urzędy certyfikacyjne (CA, wystawiające certyfikaty), urzędy rejestracyjne (RA, zbierające wnioski certyfikatów wydanie certyfikatu, weryfikują tożsamość subskrybentów), subskrybenci certyfikatów (użytkownicy, właściciele certyfikatu), oprogramowanie i sprzęt.

²⁶ W.J. Hughes Technical Center: *Public Key Infrastructure for Air Traffic Management Systems*, Federal Aviation Administration, www.icao.int/icao/en/ro/apac/ATN/SP24.pdf, 05.10.2006r.

²⁷ Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), art.6.

²⁸ Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS).

Z punktu widzenia podstawowego celu, jakim ma być usprawnienie działania systemu wizowego, należy zwrócić uwagę na fakt, że stały dostęp organów ścigania nie realizowałby tego celu. Zgodnie z art. 13 dyrektywy 95/46/WE dostęp taki może być udzielany ad hoc, w określonych okolicznościach i przy zastosowaniu odpowiednich zabezpieczeń, nie powinien to być jednak dostęp stały. Ogólnie mówiąc, przy podejmowaniu w przyszłości decyzji o udzieleniu lub nie dostępu do VIS innym organom niezbędna jest ocena proporcjonalności i konieczności²⁹.

Wskazany katalog podmiotów mających dostęp do VIS powoduje, że jest to w pewnym zakresie katalog otwarty. Determinantem, który określa możliwość dostępu do zawartych w systemie informacji, jest posiadanie kompetencji, przez organ państwa Schengen, w przedmiocie spraw wizowych i kontroli granicznych, jednakże w praktyce poszczególne państwa Schengen wprowadzają określone zmiany w zakresie podmiotowym organów uprawnionych do decydowania w sprawach wizowych. Zbyt liczna grupa podmiotów uprawnionych, nie tylko do analizy danych zawartych w systemie, ale również do ich weryfikowania i wprowadzania nowych informacji, wpływa negatywnie na konstrukcję VIS, przede wszystkim, jeśli chodzi o ochronę danych osobowych i ponoszenie odpowiedzialności ze ewentualne błędne informacje wprowadzone do systemu. Ponadto powstawać mogą wątpliwości w odniesieniu do adekwatności dostępu do danych. Przewiduje się, że jeżeli po pierwszym zapytaniu okaże się, iż dane osoby ubiegające się o wizę znajdują się w VIS (co powinno być regułą), właściwy organ może mieć dostęp do pozostałych danych, nadal w celu sprawdzenia tożsamości. Dane te dotyczą wszystkich informacji związanych z wnioskiem, fotografiami, odciskami palców, jak również z każdą uprzednio wydaną, anulowaną, cofniętą lub przedłużoną wizą. Jeżeli sprawdzenie tożsamości powiodło się, nie jest jasne, z jakiego powodu potrzebne miałyby być nadal pozostałe dane. Powinny być one udostępniane wyłącznie pod ściśle określonymi warunkami, w sytuacji, w której sprawdzenie tożsamości nie powiodło się. W takiej sytuacji dane osobowe będą wykorzystane w procedurze awaryjnej mającej na celu pomoc w ustaleniu tożsamości danej osoby. Zatem nie powinny być one dostępne dla wszystkich funkcjonariuszy przejścia granicznego.

Skomplikowana jest również sytuacja osób zidentyfikowanych jako "członkowie grupy", przez co rozumieć należy " oznaczają osoby ubiegające się o wizę, które ze względów prawnych są zobowiązane do wspólnego wjazdu na terytorium państw członkowskich i wspólnego opuszczenia tego terytorium"³⁰. Zestawiając tą definicję z definicją „wizy grupowej”, zawartą we Wspólnych Instrukcjach Konsularnych, należy stwierdzić, że terminy te nie są jednoznaczne.³¹ W przypadku członków tej samej grupy podróżnych chodzi o osoby ubiegające się o wizę, podróżujące w grupie razem z innymi osobami ubiegającymi się o wizę, np. w ramach umowy ADS (Approved Destination Status) lub razem z członkami rodziny". Precyzyjne określenie tego, kto jest członkiem tej samej grupy podróżnych ma bezpośredni związek z określeniem zasad dostępu do danych dotyczących tych osób. Chodzi

²⁹Europejski Inspektor Ochrony Danych: Opinia w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ..., (COM(2004)835 wersja ostateczna).

³⁰ Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), art. 4 pkt. 6.

³¹Dz. Urz. UE, 2005/C326/01, s.6.

o to, że w takiej sytuacji plik danych dotyczących wniosku wizowego osoby ubiegającej się o wizę będzie powiązany z plikami danych dotyczących wniosku wizowego pozostałych członków tej samej grupy podróżnych.³²

Rozporządzenie powinno zawierać dokładną i zrozumiałą definicję "członków tej samej grupy podróżnych". W obecnej formie definicja ta jest zbyt nieprecyzyjna ze względu na brak konkretnego odniesienia do Traktatu lub dorobku Schengen.

Istotnymi aktami prawnymi określającymi zasady działania VIS będą dyrektywa 95/46/WE³³, która będzie mieć zastosowanie do przetwarzania danych osobowych przez państwa Schengen dokonywanego w ramach stosowania rozporządzenia, oraz rozporządzenie 45/2001³⁴, które będzie mieć zastosowanie do działań Komisji powiązanych z ochroną danych osobowych. Stosowanie prawa krajowego zgodnie z dyrektywą 95/46/WE zazwyczaj zakłada istnienie administratora danych ustanowionego w danym państwie Schengen, natomiast stosowanie rozporządzenia 45/2001 zależy od przetwarzania danych osobowych³⁵ przez instytucję lub organ Wspólnoty w ramach wykonywania czynności, których część lub całość jest objęta zakresem prawa wspólnotowego.

W tym kontekście powstaje pytanie o rolę Komisji w obszarze funkcjonowania VIS. Dane mają być bowiem przetwarzane przez VIS w imieniu państwa Schengen. Zgodnie z art. 41 państwa Schengen wyznaczają organy traktowane jako administratorów danych³⁶. Wydaje się zatem, iż Komisja powinna być uważana za przetwarzającego³⁷. Trudno dokładnie połączyć rolę Komisji z pojęciem administratora danych lub przetwarzającego. Albo jest ona przetwarzającym posiadającym nadzwyczajne uprawnienia (w tym również do tworzenia

³² Rozp. Parlamentu Europejskiego i Rady (WE) NR 767/2008 z dn. 09.07.2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS).

³³ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dn. 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz. U. L 281 z 23.11.1995r.

³⁴ Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. w sprawie ochrony osób prywatnych w odniesieniu do postępowania z danymi osobowymi przez instytucje i organy wspólnotowe oraz w sprawie swobodnego przepływu tych danych Dziennik Urzędowy L 8/1 z 12.01.2001r.

³⁵ „przetwarzanie danych osobowych” („przetwarzanie”) oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie.

³⁶ „administrator danych” - oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, który samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych; jeżeli cele i sposoby przetwarzania danych są określone w przepisach ustawowych i wykonawczych lub przepisach wspólnotowych, administrator danych może być powoływany lub kryteria jego powołania mogą być ustalone przez ustawodawstwo krajowe lub wspólnotowe. Dyrektywa 95/46/WE, art. 2 lit. d.

³⁷ „przetwarzający” - oznacza osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych.

systemu) lub administratorem danych posiadającym ograniczone uprawnienia (zważywszy, że dane są wprowadzane i wykorzystywane przez państwa Schengen)³⁸. Ta istotna rola powinna zostać uznana poprzez zrozumiałe opisanie zadań Komisji, a nie poprzez używanie sformułowań, które niezupełnie odpowiadają rzeczywistości, ponieważ wydają się być zbyt restrykcyjne, przez co nie zmieniają niczego w korzystaniu z VIS, a jedynie prowadzą do nieporozumień. Jest to również istotne ze względu na spójny i skuteczny nadzór nad VIS.

Zadania nadzoru nad VIS rozdzielone są pomiędzy krajowe organy nadzorcze oraz EIOD. Krajowe organy nadzorcze monitorują zgodność z prawem przetwarzania danych osobowych przez państwa Schengen, w tym przesyłanie tych danych do i z VIS. EIOD monitoruje działania Komisji, w tym zapewnienie tego, by dane osobowe przesyłane były w sposób zgodny z prawem pomiędzy interfejsami krajowymi i Centralnym Systemem Informacji Wizowej. To może skutkować pokrywaniem się kompetencji, jako że zarówno krajowy organ nadzorczy jak i EIOD w tym samym czasie są odpowiedzialni za monitorowanie zgodności z prawem przesyłania danych pomiędzy interfejsami krajowymi i Centralnym Systemem Informacji Wizowej. Istotne jest podkreślenie, że działania w zakresie nadzoru prowadzone przez krajowe organy nadzorcze i EIOD powinny być skoordynowane celem zapewnienia wystarczającego poziomu spójności i ogólnej skuteczności.

4. WNIOSKI

Dalszy rozwój wspólnej polityki wizowej wymaga skutecznej wymiany odpowiednich danych. VIS jest jednym z mechanizmów, który może zapewnić niezakłócony przepływ informacji. Wydaje się, że istnieją wystarczające powody uzasadniające utworzenie VIS w celu usprawnienia wspólnej polityki wizowej. Uznać należy korzyści płynące z wykorzystania danych biometrycznych, ale jednocześnie podkreślenia wymagają poważne konsekwencje wynikające z ich wykorzystania. Dlatego pożądane jest wprowadzenie bardziej rygorystycznych ograniczeń w tym zakresie. Ponadto niedoskonałości techniczne w odniesieniu do wykorzystania danych biometrycznych wymagają ustanowienia procedur awaryjnych. Konieczne wydaje się również konieczne bardziej jednolite określenie kryteriów jakimi kierować się mają państwa członkowskie ustanawiając dla organów wewnętrznych dostęp do danych zawartych w systemie. Brak jednolitych norm postępowania w tym przedmiocie oraz niejasne zasady co do zakresu dostępnych danych mogą powodować poważne naruszenia.

Literature:

- W.J. Hughes: Public Key Infrastructure for Air Traffic Management Systems, Federal Aviation Administration, www.icao.int/icao/en/ro/apac/ATN/SP24.pdf, 2006r.
- H. Lax: Sprawozdanie delegacji komisji LIBE z wizyty w Algierii, Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Bruksela, 2006r., www.europarl.europa.eu/meetdocs/2004_2009/documents/pv/638/638724/638724pl.pdf.

³⁸ Definicja administratora danych zawarta w dyrektywie 95/46/WE i w rozporządzeniu 45/2001 przewiduje również możliwość istnienia większej liczby administratorów danych posiadających różny zakres obowiązków.

*Dávid R., Neckář J., Sehnálek D., (Editors). COFOLA 2009: the Conference Proceedings, 1. edition.
Brno : Masaryk University, 2009, ISBN 978-80-210-4821-8*

- A. Modrzejewski: Dokumenty tożsamości i systemy ewidencji ludności – rozwiązania polskie na tle rozwiązań unijnych, „Wspólnoty Europejskie” nr 5 (192) 2008, s. 30

Reviewer:

Dariusz R. Kijowski

Contact – email:

amodrzej@uwb.edu.pl