EUROPEJSKI INSPEKTOR OCHRONY DANYCH

Opinia Europejskiego Inspektora Ochrony Danych

— w sprawie wniosku dotyczącego decyzji Rady w sprawie utworzenia, działania i wykorzystania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (COM(2005)230 wersja ostateczna);

— wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie utworzenia, eksploatacji i wykorzystania Systemu Informacyjnego Schengen (SIS II) drugiej generacji (COM(2005)236 wersja ostateczna), oraz

— wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie dostępu służb odpowiedzialnych w Państwach Członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II) (COM(2005)237 wersja ostateczna)

(2006/C 91/11)

EUROPEJSKI INSPEKTOR OCHRONY DANYCH,

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

uwzględniając Kartę Praw Podstawowych Unii Europejskiej, w szczególności 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 art. 41,

uwzględniając wniosek w sprawie opinii zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 otrzymany od Komisji w dniu 17 czerwca 2005 r.;

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1. WSTĘP

1.1. Kontekst

System Informacyjny Schengen („SIS") stanowi obejmujący terytorium całej UE system informatyczny utworzony jako środek wyrównawczy po zniesieniu kontroli na granicach wewnętrznych obszaru Schengen. SIS umożliwia właściwym organom w państwach członkowskich wymianę informacji wykorzystywanych w celu przeprowadzania kontroli osób i przedmiotów na granicach zewnętrznych lub na terytorium UE, a także w celu wydawania wiz i dokumentów pobytowych.

Konwencja z Schengen weszła w życie w roku 1995 jako umowa międzyrządowa. SIS, jako część konwencji z Schengen, został następnie włączony w ramy UE traktatem z Amsterdamu.

Nowy System Informacyjny Schengen II „drugiej generacji" zastąpi obecny system umożliwiając tym samym rozszerzenie obszaru Schengen na nowe państwa członkowskie UE. Zostaną również wprowadzone do niego nowe funkcje. Przepisy dotyczące Schengen, opracowane w ramach współpracy międzyrządowej, zostaną przekształcone w pełni w klasyczne instrumenty prawodawstwa europejskiego.

Dnia 1 czerwca 2005 r. Komisja Europejska przedłożyła trzy wnioski dotyczące utworzenia SIS II. Są to:

— wniosek dotyczący rozporządzenia opartego na tytule IV traktatu WE (wizy, azyl, imigracja oraz inne polityki związane ze swobodnym przepływem osób), obejmującego aspekty SIS II należące do pierwszego filaru (imigracja), dalej zwany „wnioskiem dotyczącym rozporządzenia";

— wniosek dotyczący decyzji opartej na tytule VI traktatu UE (współpraca policyjna i sądowa w sprawach karnych), obejmującej aspekty SIS II należące do trzeciego filaru, dalej zwany „wnioskiem dotyczącym decyzji";

— wniosek dotyczący rozporządzenia opartego na tytule V (transport), poświęcony dostępowi organów odpowiedzialnych za rejestrację pojazdów do danych zawartych w SIS; ten wniosek zostanie omówiony osobno (zob. pkt 4.6 poniżej).

W tym kontekście warto wspomnieć, że w najbliższych miesiącach Komisja wyda komunikat dotyczący interoperacyjności i pogłębionej synergii pomiędzy systemami informacyjnymi UE (SIS, VIS, Eurodac).

SIS II składa się z centralnej bazy danych zwanej „Centralnym Systemem Informacyjnym Schengen" (CS-SIS), dla którego Komisja zapewnia zarządzanie operacyjne, powiązanej z krajowymi punktami dostępu określonymi przez każde państwo członkowskie (NI-SIS). Organy SIRENE zapewniają wymianę wszelkich informacji uzupełniających (informacje związane z wpisami do SIS II, ale nie zachowywane w SIS II).

Państwa członkowskie będą przekazywać do SIS II dane dotyczące osób poszukiwanych w celu aresztowania, wydania lub ekstradycji, w celu przeprowadzenia procedur sądowych, osób mających być umieszczone pod nadzorem lub wymagających szczególnych kontroli, osób, którym należy odmówić wjazdu na granicy zewnętrznej oraz przedmiotów zagubionych lub ukradzionych. Zespół danych zwany „wpisem" wprowadzony do SIS umożliwia właściwemu organowi identyfikację danej osoby lub przedmiotu.

W SIS II rozwinięto nowe cechy: poszerzony dostęp do SIS (Europol, Eurojust, prokuratorzy krajowi, organy odpowiedzialne za rejestrację pojazdów), wzajemne połączenia pomiędzy wpisami, dodanie nowych kategorii danych, w tym danych biometrycznych (odciski palców i zdjęcia) oraz platforma techniczna dzielona z Systemem Informacji Wizowej. Te nowe funkcje wywołały trwające już lata dyskusje na temat zmiany celu SIS, który z narzędzia kontroli ma się przekształcić w system sprawozdawczy i śledczy.

1.2. **Ogólna ocena wniosków**

1. Europejski Inspektor Ochrony Danych (EIOD) przyjmuje z zadowoleniem wniosek o wydanie opinii na podstawie art. 28 ust. 2 rozporządzenia (WE) nr 45/2001. Jednak uwzględniając wiążący charakter art. 28 ust. 2, niniejsza opinia powinna zostać wspomniana w preambule omawianych tekstów.

2. Istnieje kilka przyczyn, dla których EIOD z zadowoleniem przyjmuje omawiane wnioski. Przekształcenie struktury międzyrządowej w instrumenty prawodawstwa europejskiego ma kilka pozytywnych konsekwencji: zostanie wyjaśniona wartość prawna zasad rządzących SIS II (Trybunał Sprawiedliwości będzie właściwy do celów interpretacji instrumentu prawnego dotyczącego pierwszego filaru), Parlament Europejski zostanie przynajmniej częściowo zaangażowany w proces (choć na dość późnym etapie).

3. Ponadto, co do treści, istotne partie omawianych wniosków dotyczą ochrony danych i w części zawierają one zadowalające zmiany w stosunku do sytuacji obecnej. W szczególności należy wspomnieć środki na rzecz ofiar kradzieży tożsamości, rozszerzenie zakresu rozporządzenia 45/2001 na przetwarzanie danych osobowych przez Komisję w ramach działalności objętej tytułem VI oraz lepszą definicję podstaw wprowadzania wpisów dotyczących osób w celu odmowy wjazdu.

4. Jest również oczywiste, że podczas redagowania wniosków wykazano się wielką starannością; teksty są złożone, jednak odzwierciedla to złożoność systemu, do którego się odnoszą. Większość uwag zawartych w niniejszej opinii ma na celu wyjaśnienie lub uzupełnienie przepisów, co jednak nie będzie wymagało całkowitego przeredagowania tekstów.

Mimo tych ogólnie rzecz biorąc pozytywnych uwag należy podnieść kilka zastrzeżeń w szczególności do następujących kwestii:

1. Pod wieloma względami trudno jest określić, jakie były intencje autorów tekstu; przydatne byłoby załączenie uzasadnienia. Biorąc pod uwagę skomplikowanie omawianych dokumentów wydaje się to jedna z podstawowych kwestii. Brak uzasadnienia w niektórych przypadkach nie pozostawia czytelnikowi innej alternatywy jak zgadywanie.

2. Ponadto z żalem stwierdza się brak studium oceny oddziaływania. Tego braku nie uzasadnia fakt, że pierwsze wersja systemu już działa, gdyż pomiędzy obiema wersjami występują znaczące różnice. Między innymi należałoby lepiej przemyśleć oddziaływanie wprowadzenia danych biometrycznych.

3. Ramy prawne ochrony danych są wysoce skomplikowane; opierają się one na połączonym stosowaniu *lex generalis* i *lex specialis*. Należy zapewnić pełne zastosowanie istniejących ram prawnych ochrony danych ustanowionych dyrektywą 95/46/WE i rozporządzeniem 45/2001 nawet po opracowaniu szczegółowych aktów prawnych w tej dziedzinie. Połączone stosowanie różnych instrumentów prawnych nie powinno prowadzić ani do rozbieżności w zasadniczych kwestiach pomiędzy systemami krajowymi, ani do obniżenia obecnego poziomu ochrony danych.

4. Dostęp do danych dla wielu nowych organów, niemieszczących się w ramach pierwotnego „celu kontroli osób i przedmiotów", powinien być obwarowany ściślejszymi zabezpieczeniami.

5. Wnioski w istotnej części są oparte na innych instrumentach prawnych, nad którymi nadal toczą się prace (czasami nie istnieją nawet dotyczące ich wnioski). EIOD rozumie trudności wiążące się z tworzeniem prawa w tak złożonym i ciągle zmieniającym się środowisku; mimo to, mając na względzie skutki, jakie mogą ponieść zainteresowane osoby oraz związany z powyższym brak pewności prawnej, uważa, że taka sytuacja jest nie do przyjęcia.

6. Nie do końca określony jest podział kompetencji pomiędzy państwami członkowskimi a Komisją. Jasność jest wartością podstawową, konieczną nie tylko do sprawnego funkcjonowania systemu, ale także wymaganą w celu zapewnienia całościowego nadzoru nad systemem.

1.3. **Struktura opinii**

Opinia ma następującą strukturę: po pierwsze, wyjaśnia podstawy prawne mające zastosowanie do SIS II. Następnie przechodzi do określenia celu SIS II oraz elementów, które znacząco różnią się od aktualnego systemu. W pkt 5 zawarto uwagi na temat ról odgrywanych odpowiednio przez Komisję i państwa członkowskie w funkcjonowaniu SIS II. Pkt 6 dotyczy praw osoby, której dotyczą dane, zaś pkt 7 dotyczy nadzoru na szczeblu krajowym i przeprowadzanego przez EIOD oraz współpracy pomiędzy nadzorującymi. Pkt 8 zawiera kilka uwag i propozycji możliwych zmian w kwestii bezpieczeństwa; pkt 9 i 10 dotyczą odpowiednio komitologii i interoperacyjności. Na końcu, we wnioskach podkreślono najważniejsze konkluzje płynące z każdego z punktów.

2. ISTOTNE RAMY PRAWNE

2.1. **Istotne ramy ochrony danych zawartych w SIS II**

Wniosek odwołuje się do dyrektywy 95/46/WE, konwencji 108 i rozporządzenia 45/2001 jako podstaw prawnych dotyczących ochrony danych. Istotne są również inne instrumenty.

W celu wyjaśnienia kontekstu i przypomnienia, jakie są podstawowe punkty odniesienia naszej analizy, należy wymienić następujące zagadnienia:

— W Europie poszanowanie życia prywatnego jest zapewnione od momentu przyjęcia w 1950 r. Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (zwanej dalej: „europejską konwencją praw człowieka" lub EKPC) przez Radę Europy. Art. 8 EKPC ustanawia „prawo do poszanowania życia prywatnego i rodzinnego".

  Zgodnie z art. 8 ust. 2 jakakolwiek ingerencja władzy publicznej w korzystanie z tego prawa jest dozwolona wyłącznie, jeżeli jest „przewidziana przez ustawę" oraz „konieczna w demokratycznym społeczeństwie" z uwagi na ochronę ważnych interesów. Według orzecznictwa Europejskiego Trybunału Praw Człowieka warunki te spowodowały konieczność ustanowienia dodatkowych wymogów, takich jak: rodzaj podstawy prawnej dla ingerencji, proporcjonalność środków i konieczność odpowiedniego zabezpieczenia przed nadużyciami.

— Prawo do poszanowania życia prywatnego oraz ochrona danych osobowych zostały umieszczone później w art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej. Zgodnie z art. 52 karty przewiduje się możliwość ograniczenia tych praw, o ile są spełnione warunki podobne do tych, które przewiduje art. 8 konwencji o ochronie praw człowieka.

— Artykuł 6 ust. 2 traktatu o UE stanowi, że Unia respektuje prawa podstawowe gwarantowane w EKPC.

Trzy teksty mające bezpośrednie zastosowanie do wniosków dotyczących SIS II to:

— Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych (zwana dalej *„konwencją 108"*) określiła podstawowe zasady ochrony osób z związku z przetwarzaniem danych osobowych. Wszystkie państwa członkowskie ratyfikowały konwencję 108. Ma ona zastosowanie również do działań w obszarze policji i wymiaru sprawiedliwości. Konwencja 108 stanowi aktualnie podstawę systemu ochrony danych mającego zastosowanie do konwencji SIS wraz z rekomendacją nr R (87) 15 Komitetu Ministrów Rady Europy z dnia 17 września 1987 r. dotyczącą ochrony danych osobowych wykorzystywanych w sektorze policji.

— dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz.U. L 281, str. 31). Dyrektywa ta będzie dalej nazywana *„dyrektywą 95/46/WE"*. Należy zauważyć, że w większości państw członkowskich prawo krajowe wdrażające tę dyrektywę obejmuje również przetwarzanie danych w obszarze policji i wymiaru sprawiedliwości.

— 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 (Dz.U. L 8, str. 1). Rozporządzenie to będzie dalej nazywane *„rozporządzeniem 45/2001"*.

Interpretacja dyrektywy 95/46/WE i rozporządzenia 45/2001 musi po części zależeć od właściwego orzecznictwa Europejskiego Trybunału Praw Człowieka zgodnie z europejską konwencją praw człowieka (EKPC) z 1950 r. Innymi słowy, dyrektywa i rozporządzenie, w zakresie w jakim dotyczą przetwarzania danych osobowych mogącego prowadzić do naruszeń podstawowych wolności, a zwłaszcza prawa do prywatności, muszą być interpretowane w świetle praw podstawowych. Powyższe wynika również z orzecznictwa Europejskiego Trybunału Sprawiedliwości ([1]).

([1]) W tym kontekście należy zrobić odniesienie do wyroku Trybunału Sprawiedliwości w sprawie Österreichischer Rundfunk i inni (sprawy połączone C-465/00, C-138/01 oraz C-139/01, wyrok z dnia 20 maja 2003 r., sąd w pełnym składzie, (2003) Zb.Orz. I-4989). Trybunał zajął się austriacką ustawą dotyczącą transferu informacji o wynagrodzeniu pracowników w sektorze publicznym do austriackiego sądu obrachunkowego i ich późniejszą publikacją. W wyroku Trybunał ustala kryteria, opracowane na podstawie art. 8 europejskiej konwencji praw człowieka, do których należy się odwoływać przy stosowaniu dyrektywy 95/46/WE w takim zakresie, w jakim dyrektywa ta pozwala na pewne ograniczenia prawa do prywatności.

Dnia 4 października 2005 r. Komisja przedłożyła wniosek dotyczący decyzji ramowej Rady w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych ([1]) (dalej zwany *„projektem decyzji ramowej"*). Ta decyzja ramowa ma zastąpić konwencję 108 jako prawna rama odniesienia dla projektu decyzji o SIS II, która prawdopodobnie w tym kontekście będzie miała wpływ na system ochrony danych (zob. pkt 2.2.5 poniżej).

2.2. **System prawny ochrony danych SIS II**

2.2.1. *Uwaga ogólna*

Podstawa prawna niezbędna do zarządzania SIS II składa się z osobnych instrumentów; mimo to, jak określono w motywach, „nie narusza zasady, zgodnie z którą SIS II stanowi jeden odrębny system informacyjny, który powinien działać jako taki. Niektóre postanowienia tych instrumentów powinny być zatem identyczne".

Struktura obydwóch omawianych dokumentów jest zasadniczo taka sama, przy czym rozdziały I-III w obydwu tekstach są właściwie identyczne. Fakt, że SIS II ma być postrzegany jako jeden system informacyjny oparty na dwu podstawach prawnych ma odzwierciedlenie w dość skomplikowanym systemie ochrony danych.

System ochrony danych został określony po części w samych wnioskach jako „*lex specialis*", uzupełniony przez różne akty prawne służące jako odniesienie („*lex generalis*") dla każdego sektora (Komisja, państwa członkowskie w pierwszym filarze, państwa członkowskie w trzecim filarze).

Taka struktura powoduje pytanie o sposób podejścia do wyspecjalizowanych zbiorów zasad w odniesieniu do prawa ogólnego. W tym przypadku EIOD uważa zasady szczegółowe za zastosowanie zasady ogólnej. W konsekwencji *lex specialis* musi zawsze być zgodne z *lex generalis*; rozwija ono *lex generalis* (uszczegóławia je lub dodaje elementy), ale nie stanowi wyjątku od niego.

Co do tego, jaka zasada powinna być stosowana w danym przypadku, pierwszeństwo ma *lex specialis*, lecz w wypadku jego braku lub niejasności, należy poczynić odniesienie do *lex generalis*.

Zgodnie z tą strukturą są możliwe trzy różne kombinacje *lex generalis* i *lex specialis*. Można je podsumować w następujący sposób.

2.2.2. *System mający zastosowanie do Komisji*

Gdy zaangażowana jest Komisja, ma zastosowanie rozporządzenie 45/2001, również w tym, co dotyczy roli EIOD, niezależnie od tego, czy prowadzone działania należą do pierwszego (wniosek dotyczący rozporządzenia) czy trzeciego (wniosek dotyczący decyzji) filaru. Motyw 21 wniosku dotyczącego decyzji mówi: „Rozporządzenie (WE) nr 45/2001 (…) ma zastosowanie do przetwarzania danych osobowych przez Komisję, gdy przetwarzanie to odbywa się w ramach działalności, która w całości lub części wchodzi w zakres prawa wspólnotowego. Częściowo przetwarzanie danych osobowych w SIS II wchodzi w zakres prawodawstwa wspólnotowego."

Istnieją dla tego praktyczne powody: w przypadku Komisji byłoby niezwykle trudne ustalenie, czy dane są przetwarzane w ramach działań objętych prawodawstwem dotyczących pierwszego czy też trzeciego filaru.

Ponadto zastosowanie jednego instrumentu prawnego do wszystkich działań Komisji w kontekście SIS II nie tylko jest bardziej zasadne z praktycznego punktu widzenia, ale też poprawia spójność (zapewniając, zgodnie z motywem 21 wniosku dotyczącego zaproponowanego rozporządzenia „spójne i jednolite stosowanie przepisów dotyczących ochrony podstawowych praw i swobód osób fizycznych w zakresie przetwarzania danych osobowych"). Dlatego też EIOD z zadowoleniem przyjmuje uznanie przez Komisję, że rozporządzenie 45/2001 ma zastosowanie do wszelkiej działalności Komisji związanej z przetwarzaniem danych w SIS II.

2.2.3. *System mający zastosowanie do państw członkowskich*

Sytuacja państw członkowskich jest bardziej skomplikowana. Przetwarzanie danych osobowych w ramach stosowania wniosku dotyczącego rozporządzenia podlega samemu temu wnioskowi oraz dyrektywie 95/46/WE. Lektura motywu 14 wniosku dotyczącego rozporządzenia nie pozostawia wątpliwości, że dyrektywę należy uważać za *lex generalis*, zaś rozporządzenie o SIS II za *lex specialis*. Niesie to za sobą skutki przedstawione poniżej.

Co do wniosku dotyczącego decyzji, stanowiącym odniesienie instrumentem prawnym dotyczącym ochrony danych (*lex generalis*) jest konwencja 108, co pociąga za sobą istotne różnice w niektórych punktach systemów ochrony danych odnoszących się do pierwszego i trzeciego filaru.

2.2.4. *Wpływ na poziom ochrony danych*

Jako ogólny komentarz do architektury ochrony danych EIOD podkreśla następujące kwestie:

— Zastosowanie wniosku dotyczącego rozporządzenia jako *lex specialis* w stosunku do dyrektywy 95/46/WE (i, podobnie, zastosowanie wniosku dotyczącego decyzji jako *lex specialis* w stosunku do konwencji 108) nie powinno w żadnym wypadku prowadzić do obniżenia poziomu ochrony danych zapewnianego na mocy tej dyrektywy lub konwencji. EIOD sporządzi w tym celu odpowiednie zalecenia (zob. na przykład prawo do środków odwoławczych).

([1]) (COM (2005) 475 wersja ostateczna).

— Podobnie, wynikiem połączonego stosowania instrumentów prawnych nie może być obniżenie poziomu ochrony danych zapewnionego na mocy obowiązującej konwencji z Schengen (zob. na przykład uwagi dot. art. 13 dyrektywy 95/46/WE zamieszczone poniżej).

— Zastosowanie dwóch różnych instrumentów, choć konieczne ze względu na ramy prawa europejskiego, nie powinno prowadzić do nieuzasadnionych rozbieżności pomiędzy ochroną danych osób, których te dane dotyczą w zależności od typu przetwarzanych danych. Należy tego w miarę możliwości unikać. Poniższe zalecenia mają również na celu zapewnienie jak największej spójności (zob. na przykład uprawnienia krajowych organów nadzorczych).

— Ramy prawne są tak złożone, że bardzo prawdopodobne jest zajście nieporozumień podczas ich praktycznego stosowania. W niektórych przypadkach trudno jest zauważyć sposób współdziałania *lex generalis* i *lex specialis* i zasadne byłoby jego wyjaśnienie w omawianych wnioskach. Ponadto, w tym skomplikowanym środowisku prawnym, bardzo pomocna jest sugestia ze strony wspólnego organu nadzorczego Schengen wyrażona w opinii dotyczącej proponowanej podstawy prawnej dla SIS II (z 27 września 2005 r.), by opracować „vademecum" wymieniające wszystkie istniejące prawa mające związek z SIS II wraz z jasno określoną hierarchią możliwych do zastosowania aktów prawnych.

Podsumowując, niniejsza opinia będzie miała na celu zapewnienie wysokiego poziomu ochrony danych, spójności i jasności w celu zapewnienia osobie, której dotyczą przetwarzane dane, niezbędnej pewności prawnej.

2.2.5. *Wpływ projektu decyzji ramowej na ochronę danych w obrębie trzeciego filaru*

Konwencja 108 jako stanowiący odniesienie instrument dotyczący ochrony danych dla projektu decyzji o SIS II zostanie zastąpiona przez decyzję ramową w sprawie ochrony danych w trzecim filarze ([1]). Nie wspomniano o tym we wniosku, ale wynika to z wniosku dotyczącego decyzji ramowej. Jego art. 34 ust. 2 stanowi, że „wszelkie odniesienia do konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r. należy rozumieć jako odniesienia do niniejszej decyzji ramowej". EIOD w najbliższych tygodniach wyda opinię dotyczącą projektu decyzji ramowej i z tego też powodu nie przeprowadzi jej szczegółowej analizy w niniejszej opinii. Mimo to w miejscach, w których zastosowanie decyzji ramowej prawdopodobnie znacząco wpłynie na system ochrony danych SIS II, zostanie to jasno wspomniane.

2.2.6. *Stosowanie art. 13 dyrektywy 95/46/WE oraz art. 9 konwencji 108*

Art. 13 dyrektywy 95/46/WE oraz art. 9 konwencji 108 dają państwom członkowskim możliwość podjęcia środków legislacyjnych w celu zawężenia zakresu obowiązków i praw w nich przewidzianych, gdy takie ograniczenie stanowi środek konieczny do ochrony innych ważnych interesów (np. bezpieczeństwa narodowego, obrony, bezpieczeństwa publicznego) ([2]).

W motywach obydwu wniosków dotyczących rozporządzenia i decyzji wspomina się o tym, że państwa członkowskie mogą skorzystać z tej możliwości podczas wdrażania wniosków na poziomie krajowym. W takim przypadku należy zastosować podwójne sprawdzenie: zastosowanie art. 13 dyrektywy 95/46/WE musi być zgodne z art. 8 EKPC oraz nie powinno prowadzić do obniżenia obecnego poziomu ochrony danych.

Jest to tym bardziej istotne w przypadku SIS II, gdyż system musi być przewidywalny. Jako że państwa członkowskie mają dostęp do danych, musi istnieć możliwość w miarę pewnego poznania sposobu ich przetwarzania na szczeblu krajowym.

Obawy budzi zwłaszcza jeden element, gdyż wnioski mogłyby z jego powodu doprowadzić do obniżenia dotychczasowego poziomu ochrony danych. Art. 102 konwencji z Schengen przewiduje system, w którym wykorzystanie danych jest ściśle uregulowane i ograniczone, nawet w prawie krajowym („Wszelkie wykorzystanie danych, które nie jest zgodne z ustępami 1-4, uznaje się za niewłaściwe wykorzystanie zgodnie z prawem krajowym każdej z Umawiających się Stron."). Zarówno dyrektywa 95/46/WE, jak i konwencja 108 przewidują jednak możliwość wprowadzenia wyjątków, między innymi od zasady ograniczenia celu, do prawa krajowego. Skorzystanie z tej możliwości stanowiłoby rozbieżność w stosunku do obecnego systemu przewidzianego konwencją z Schengen, zgodnie z którą ustawodawstwo krajowe nie może odbiegać od fundamentalnej zasady ograniczenia celu i zakresu wykorzystania.

Przyjęcie decyzji ramowej nie zmieniłoby powyższego; problemem jest raczej utrzymanie zasady ścisłego ograniczenia celu w odniesieniu do przetwarzania danych SIS II niż zapewnienie, że dane będą przetwarzane zgodnie z decyzją ramową.

([1]) Zastąpi ona również ogólny system ochrony danych z konwencji z Schengen (art. 126-130 konwencji z Schengen). Ten system nie ma zastosowania do SIS.

([2]) Państwo członkowskie wykorzystujące opcję ograniczenia praw może to zrobić tylko w zgodności z art. 8 EKPC, jak wspomniano wcześniej.

EIOD proponuje wprowadzenie do wniosków dotyczących SIS II (tj. do art. 21 wniosku dotyczącego rozporządzenia oraz do art. 40 wniosku dotyczącego decyzji) przepisu o skutku równoważnym skutkowi art. 102 ust. 4 konwencji z Schengen, ograniczającego możliwość wykorzystywania przez państwa członkowskie danych nieprzewidzianych w tekstach dotyczących SIS II. Inną możliwością jest jednoznaczne ograniczenie we wniosku dotyczącym decyzji oraz we wniosku dotyczącym rozporządzenia zakresu wyjątków, które mogą zostać zastosowane zgodnie z art. 13 dyrektywy lub art. 6 konwencji, określając na przykład, że państwa członkowskie mogą ograniczyć wyłącznie prawa dostępu i informacji, lecz nie zasady jakości danych.

3. **CEL**

Zgodnie z art. 1 obydwu omawianych dokumentów („Utworzenie i ogólny cel SIS II") SIS II jest tworzony „celem umożliwienia właściwym organom państw członkowskich wymiany informacji do celów kontroli osób i przedmiotów" oraz „przyczynia się do utrzymania wysokiego poziomu bezpieczeństwa w obszarze bez kontroli granic wewnętrznych pomiędzy państwami członkowskimi".

Cel SIS II został określony w sposób dość schematyczny; powyższe przepisy same w sobie nie określają precyzyjnie, co ten cel obejmuje (oznacza).

Cel SIS II wydaje się dużo szerszy niż cel obecnego SIS, określony w art. 92 konwencji z Schengen, który odnosi się szczególnie do „(…) dostępu do wpisów dotyczących osób i majątku w celach kontroli granicznej oraz innych kontroli policyjnych i celnych (…) oraz, w przypadku szczególnej kategorii wpisów, określonych w art. 96, w celach wydawania wiz, dokumentów pobytowych i wykonywania przepisów prawnych o cudzoziemcach (…)".

Ten szerszy cel wynika również z dodania do SIS II nowych funkcji i możliwości dostępu, które nie są zgodne z pierwotnym celem kontroli osób i przedmiotów, lecz raczej charakteryzują narzędzie śledcze. W szczególności przewidziano dostęp dla organów, które będą wykorzystywać dane SIS II dla własnych celów, nie zaś dla realizacji celów SIS II (zob. poniżej); powszechne będą wzajemne połączenia pomiędzy wpisami, co jest typową cechą policyjnych narzędzi śledczych.

Nasuwają się także pytania związane z wyszukiwarką biometryczną, która ma zostać opracowana w najbliższych latach, umożliwiając przeszukiwanie systemu, co wykracza poza potrzeby systemu kontroli.

Podsumowując, zakres omawianych wniosków jest o wiele szerszy od zakresu istniejących ram prawnych. Wymaga to dodatkowych zabezpieczeń. W związku z tym EIOD skupi swą analizę raczej na funkcjach i innych elementach składowych SIS II niż na samej szerokiej definicji zawartej w art. 1.

4. **ZNACZĄCE ZMIANY W SIS II**

W tym rozdziale skupiono się przede wszystkim na nowych elementach, które wnosi ze sobą SIS II, mianowicie na wprowadzeniu danych biometrycznych, nowej koncepcji dostępu, szczególnie dostępu dla Europolu i Eurojustu oraz organów odpowiedzialnych za rejestrację pojazdów, wzajemnych powiązaniach między wpisami oraz na dostępie różnych organów do danych dotyczących imigracji.

4.1. **Dane biometryczne**

Wnioski dotyczące SIS II wprowadzają możliwość przetwarzania nowej kategorii danych, która wymaga szczególnej uwagi: danych biometrycznych. Jak EIOD podkreślił w swojej wcześniejszej opinii dotyczącej Systemu Informacji Wizowej ([1]), wrażliwy charakter danych biometrzycznych wymaga szczególnych zabezpieczeń, które nie zostały ujęte we wnioskach dotyczących SIS II.

Ogólnie rzecz biorąc, tendencja do wykorzystywania danych biometrycznych w obejmujących całe terytorium UE systemach informacyjnych (VIS, EURODAC, system informacji o prawach jazdy itd.) stale rośnie, nie towarzyszy jej jednak szczegółowa refleksja dotycząca związanego z tymi systemami ryzyka oraz wymaganych zabezpieczeń.

Ta potrzeba głębszej refleksji została również podkreślona w ostatniej rezolucji z Międzynarodowej Konferencji Rzeczników Ochrony Danych w Montreux ([2]) dotyczącej danych biometrycznych. Jak dotąd wartość dodana opracowywania norm była skupiona wyłącznie na rosnącej interoperacyjności pomiędzy systemami, nie zaś na poprawie jakości procesów biometrycznych.

([1]) Opinia EIOD 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, 23 marca 2005 r., pkt 3.4.2.

([2]) 27. Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności, Montreux, 16 września 2005 r., Rezolucja w sprawie zastosowania danych biometrycznych w paszportach, dokumentach tożsamości oraz dokumentach podróży.

Wskazane byłoby stworzenie zestawu wspólnych obowiązków lub wymogów związanych ze specyfiką tych danych, a także wspólnej metodologii ich wdrażania. Takie wspólne wymogi mogłyby zawierać w szczególności następujące elementy (ich potrzeba jest widoczna we wnioskach dotyczących SIS II):

— **nakierowana ocena oddziaływania:** należy podkreślić, że wnioski nie zostały poddane ocenie oddziaływania zastosowania danych biometrycznych ([1]).

— **nacisk na procedurę wpisywania:** źródło danych biometrycznych i sposób ich zbierania nie zostały szczegółowo opisane. Wpisywanie stanowi kluczowy element całościowego procesu identyfikacji biometrycznej i nie może zostać zdefiniowany wyłącznie w załącznikach lub podczas dalszych dyskusji w podgrupach, gdyż bezpośrednio warunkuje ono końcowe rezultaty procesu, tj. poziom błędu fałszywego odrzucenia (FRR) lub błędu fałszywego przyjęcia (FAR).

— **podkreślenie poziomu dokładności:** wykorzystanie danych biometrycznych w celu identyfikacji (porównywanie jednostki ze zbiorem) przedstawione we wnioskach jako przyszłe wdrożenie „wyszukiwarki biometrycznej" jest problematyczne, gdyż wyniki tego procesu są mniej dokładne niż wykorzystanie danych biometrycznych w celu uwierzytelnienia lub kontroli (porównywanie jednostki z jednostką). Identyfikacja biometryczna nie powinna więc stanowić jedynego sposobu identyfikacji lub jedynego klucza dostępu do informacji.

— **procedura awaryjna:** powinny zostać wdrożone gotowe do wykorzystania procedury awaryjne mające na celu poszanowanie godności osób, które mogły zostać błędnie zidentyfikowane, oraz uniknięcie przerzucenia na te osoby ciężaru niedoskonałości systemu.

Wykorzystanie danych biometrycznych bez właściwej uprzedniej zgody zdradza również zbytnie poleganie na wiarygodności tych danych. Dane biometryczne „żyją" i ewoluują z czasem; próbki przechowywane w bazie danych stanowią jedynie zapis chwilowego stanu dynamicznego elementu. Ich aktualność nie jest absolutna i musi być kontrolowana. Dokładność danych biometrycznych musi być zawsze rozpatrywana z perspektywy innych elementów, gdyż nigdy nie jest ona wartością absolutną.

([1]) Ocena mogłaby być oparta na tzw. siedmiu filarach wiedzy o danych biometrycznych omówionych w „Biometrics at the frontiers: Assessing the impact on Society" (Dane biometryczne na granicach: ocena oddziaływania społecznego) IPTS, DG-JRC, EUR 21585 EN, część 1.2, str. 32.

Możliwe wykorzystanie danych znajdujących się w SIS II do celów śledztwa stanowi poważne ryzyko dla osoby, której dotyczą dane, jeżeli przywiązuje się większą lub nadmierną rolę do dowodów biometrycznych, jak przedstawiono w poprzednich przypadkach ([2]).

Dlatego też we wnioskach należy przedstawić faktyczne możliwości wykorzystania danych biometrycznych w celu identyfikacji oraz wpłynąć na zwiększenie zrozumienia tych możliwości.

4.2. **Dostęp do danych zawartych w SIS II**

4.2.1 *Nowa wizja dostępu*

Dla każdego wpisu określa się organy, które mają dostęp do danych SIS. Zasadniczo dla udostępnienia danych SIS stosuje się podwójne sprawdzenie: dane udostępnia się organom w pełnej zgodności z ogólnym celem SIS oraz ze szczegółowym celem każdego wpisu.

Wynika to z definicji wpisu, znajdującej się zarówno we wniosku dotyczącym rozporządzenia, jak i we wniosku dotyczącym decyzji (art. 3 ust. 1 obydwu instrumentów: *„wpis" oznacza zbiór danych wprowadzonych do SIS II umożliwiający właściwym organom zidentyfikowanie osoby lub przedmiotu w związku z konkretnym planowanym działaniem*). Art. 39 ust. 3 wniosku dotyczącego decyzji wzmacnia ten punkt widzenia, stanowiąc: *„Dane określone w ust. 1 można wykorzystywać wyłącznie w celu identyfikacji osoby w celu podjęcia szczególnego działania zgodnie z niniejszą decyzją."* Pod tym względem SIS II nadal prezentuje cechy systemu „trafienie/brak trafienia", w którym każdy wpis jest sporządzany w określonym celu (wydanie osoby, odmowa wjazdu…).

Wykorzystanie danych SIS przez organy posiadające dostęp do tych danych *de facto* podlega ograniczeniom, gdyż organy te zasadniczo mają do nich dostęp wyłącznie w celu przeprowadzenia określonych działań.

Niektóre opcje dostępu przewidziane w nowych wnioskach nie są jednak spójne z powyższym; właściwie ich celem jest zapewnienie organowi informacji, nie pozwalając mu jednak na identyfikację osoby i podjęcie działania przewidzianego we wpisie.

([2]) W czerwcu 2004 r. prawnik z Portland (USA) został na dwa tygodnie pozbawiony wolności, gdyż FBI udało się połączyć odcisk jego palca z odciskiem znalezionym do ataku terrorystycznym w Madrycie (na plastikowej torbie, która zawierała detonator). Później dowiedziono, że proces wyszukiwania zawierał usterki i że wynik końcowy był błędny.

Dotyczy to zwłaszcza:

— dostępu do danych dotyczących imigracji przez organy udzielające azylu;

— dostępu do danych dotyczących imigracji przez organy przyznające status uchodźcy;

— dostępu Europolu do wpisów o ekstradycji, niejawnym nadzorze i skradzionych dokumentach;

— dostępu do danych o ekstradycji i dotyczących miejsca pobytu przez Eurojust.

Wszystkie te organy mają te same cechy w stosunku do danych znajdujących się w SIS II:

nie są w stanie podjąć szczególnych działań określonych w definicji wpisu. Dane są im udostępniane jako źródło informacji do ich własnych celów.

Wśród tych organów należy również rozróżnić te, które mają dostęp do danych do realizacji własnych, ale raczej konkretnych celów, oraz te (mianowicie Europol i Eurojust), dla których w ogóle nie określono celu dostępu. Przykładowo organy udzielające azylu mają dostęp do danych w szczególnym celu, nawet jeżeli nie jest to cel określony we wpisie. Mogą one mieć dostęp do danych o imigracji „w celu ustalenia, czy osoba ubiegająca się o azyl przebywa nielegalnie w innym państwie członkowskim". Jednak Europol i Eurojust mają dostęp do danych zawartych w pewnych kategoriach wpisów, „co jest niezbędne do wykonywania ich zadań".

Podsumowując, dostęp do danych zawartych w SIS II jest przyznawany w trzech sytuacjach:

— dla przeprowadzenia działań przewidzianych we wpisie;

— w celu innym niż cel SIS II, lecz dobrze wpisującym się w treść wniosków;

— w celu innym niż cel SIS II, lecz niesprecyzowanym.

EIOD jest zdania, że im ogólniejszy jest cel dostępu, tym ściślejsze powinny być zabezpieczenia, jakie należy wdrożyć. Poniżej szczegółowo opisano istniejące ogólne zabezpieczenia; następnie zostanie omówiona szczególna sytuacja Europolu i Eurojustu.

4.2.2. *Warunki udzielenia dostępu*

1. W każdym przypadku dostępu udziela się wyłącznie, jeżeli jest on zgodny z ogólnym celem SIS II i spójny z jego podstawą prawną.

Oznacza to w praktyce, że dostęp do danych o imigracji zgodnie z wnioskiem dotyczącym rozporządzenia musi wspierać realizację polityk związanych z przepływem osób jako częścią dorobku prawnego Schengen.

Podobnie dostęp do wpisów określony w decyzji ma na celu wspieranie współpracy operacyjnej pomiędzy organami policji i sądownictwa w sprawach karnych.

Zgodnie z powyższym EIOD zwraca uwagę na rozdział związany z dostępem do SIS II przez służby odpowiedzialne za wydawanie dowodów rejestracyjnych (zob. pkt 4.6 poniżej).

2. Należy dowieść potrzeby dostępu do SIS II oraz niemożliwości czy znacznych trudności wiążących się ze zdobyciem danych za pomocą innych, mniej inwazyjnych środków. Powinno to zostać ujęte w uzasadnieniu, którego, jak wspomniano powyżej, niestety brakuje.

3. Sposób wykorzystania danych musi zostać jasno zdefiniowany, wraz ze wszystkimi ograniczeniami.

Na przykład organy udzielające azylu mogą mieć dostęp do danych o imigracji „w celu ustalenia, czy osoba ubiegająca się o azyl przebywa nielegalnie w innym państwie członkowskim". Jednak Europol i Eurojust mają dostęp do danych zawartych w pewnych kategoriach wpisów, „co jest niezbędne do wykonywania ich zadań": określenie do nie jest wystarczająco szczegółowe (zob. poniżej).

4. Warunki dostępu muszą być jasno zdefiniowane i ograniczone. W szczególności wewnątrz wspomnianych organizacji wyłącznie służby, które muszą korzystać z danych zawartych w SIS II, powinny mieć do nich dostęp. To zobowiązanie określone w art. 40 wniosku dotyczącego decyzji oraz w art. 21 ust. 2 wniosku dotyczącego rozporządzenia powinno zostać uzupełnione zobowiązaniem organów krajowych do sporządzenia aktualizowanej listy osób mających prawo dostępu do SIS II. To samo powinno dotyczyć Europolu i Eurojustu.

5. Fakt, że organy te mają dostęp do danych zawartych w SIS II nie może stanowić podstawy do wpisywania lub przechowywania danych w systemie, jeżeli nie są one przydatne dla wpisu, którego część stanowią. Nie można dodawać nowych kategorii danych tylko dlatego, że byłoby to z korzyścią dla innych systemów informacyjnych. Na przykład art. 39 wniosku dotyczącego decyzji przewiduje wprowadzanie do wpisów danych dotyczących organu dokonującego wpisu. Te dane nie są konieczne do wykonania działania (aresztowania, nadzoru…), a jedynym powodem ich wprowadzenia byłyby prawdopodobne korzyści dla Europolu lub Eurojustu. Należy podać jasne uzasadnienie dla przetwarzania takich danych.

6. Okres zatrzymywania danych nie może zostać przedłużony, jeżeli nie jest to konieczne do celów, dla których dokonano wpisu. Oznacza to, że nawet gdy Europol lub Eurojust mają dostęp do danych, nie jest to wystarczającym powodem, by przechowywać je w systemie (na przykład po ekstradycji osoby poszukiwanej dane powinny zostać usunięte, nawet jeżeli mogłyby być przydatne dla Europolu). Konieczny będzie szczegółowy nadzór stosowania powyższego przez organy krajowe.

4.2.3. *Dostęp Europolu i Eurojustu*

a) *Podstawy dostępu*

Dostęp Europolu i Eurojustu do niektórych danych SIS był już dyskutowany przed jego wprowadzeniem decyzją Rady z 24 lutego 2005 r. ([1]). Wśród wszystkich organów mających dostęp do danych do realizacji własnych celów Europol i Eurojust korzystają z dostępu na najbardziej liberalnych warunkach. Choć wykorzystanie tych danych zostało opisane w rozdziale XII decyzji, zwłaszcza podstawy udzielenia dostępu nie zostały wystarczająco dobrze opracowane. Sytuację pogarsza jeszcze fakt, że zadania Europolu i Eurojustu prawdopodobnie z czasem będą ewoluować.

EIOD wzywa Komisję do ścisłego zdefiniowania zadań, których wykonywanie usprawiedliwiałoby dostęp Europolu i Eurojustu do danych.

b) *Ograniczenie danych*

W celu ograniczenia „połowów informacji" przez Europol i Eurojust oraz zapewnienia, że mają one jedynie dostęp do danych „niezbędnych do wykonywania ich zadań" wspólny organ nadzorczy Schengen w opinii z dnia 27 września 2005 r. dotyczącej wniosków w sprawie SIS II zasugerował ograniczenie dostępu Europolu i Eurojustu do danych dotyczących osób, których nazwisko znajduje się już w ich aktach. To gwarantowałoby konsultowanie wyłącznie wpisów istotnych dla tych instytucji. EIOD popiera to zalecenie.

c) *Aspekty związane z bezpieczeństwem*

EIOD z zadowoleniem przyjmuje obowiązek rejestrowania wszystkich operacji przeprowadzanych w systemie przez Europol i Eurojust oraz zakaz kopiowania lub zapisywania części systemu.

Art. 56 wniosku dotyczącego decyzji przewiduje „jeden lub dwa" punkty dostępu dla Europolu i Eurojustu. Choć zrozumiałe jest, że państwo członkowskie może potrzebować więcej niż jednego punktu dostępu, ze względu na decentralizację właściwych organów, status i działalność Europolu i Eurojustu nie usprawiedliwiają takiego wniosku. Należy podkreślić również, że z punktu widzenia bezpieczeństwa mnożenie punktów dostępu zwiększa ryzyko nadużyć i dlatego powinno być ściśle i spójnie uzasadnione. Dlatego też, w obliczu braku przekonujących argumentów, EIOD proponuje zapewnić Europolowi i Eurojustowi tylko jeden punkt dostępu.

4.3. **Wzajemne powiązania między wpisami**

Art. 26 rozporządzenia i art. 46 decyzji przewidują, że państwa członkowskie mogą tworzyć połączenia pomiędzy wpisami zgodnie z prawodawstwem krajowym w celu ustanowienia związku pomiędzy dwoma lub więcej wpisami.

Chociaż połączenia pomiędzy wpisami mogą z pewnością być użyteczne dla kontroli (np. nakaz aresztowania złodzieja samochodów może być połączony z wpisem dotyczącym skradzionego pojazdu), wprowadzenie takich połączeń jest bardzo typową cechą policyjnych narzędzi śledczych.

Połączenia między wpisami mogą mieć większy wpływ na prawa osoby, której dotyczą, gdyż osoba ta nie będzie dłużej „oceniania" na podstawie danych odnoszących się bezpośrednio do niej, lecz na podstawie jej możliwych powiązań z innymi osobami. Osoby, których dane zostały powiązane z danymi dotyczącymi przestępców lub osób poszukiwanych, mogą być traktowane z większą nieufnością niż inne. Ponadto połączenia między wpisami stanowią przedłużenie możliwości dochodzeniowych SIS, gdyż umożliwią rejestrowanie domniemanych band lub sieci (jeżeli, na przykład, dane dotyczące nielegalnych imigrantów zostaną połączone z danymi dotyczącymi handlarzy ludźmi). W dodatku konsekwencją faktu, że ustanawianie połączeń pozostawiono w gestii prawodawstwa krajowego może być to, że połączenia niezgodne z prawem w jednym państwie członkowskim będą ustanawiane przez inne państwo, w ten sposób powodując wprowadzenie „nielegalnych" danych do systemu.

([1]) Decyzja Rady 2005/211/WSiSW z dnia 24 lutego 2005 r. dotycząca wprowadzenia kilku nowych funkcji do Systemu Informacyjnego Schengen, w tym związanych z walką z terroryzmem, Dz.U. L 68/44 z 15.3.2005

Konkluzje Rady z dnia 14 czerwca 2004 r. dotyczące wymogów funkcjonalnych SIS II stanowiły, że każde połączenie musi odpowiadać jasnemu wymogowi operacyjnemu, być oparte na jasno określonych związkach i być zgodne z zasadą proporcjonalności. Ponadto połączenia nie mogą wpływać na prawo dostępu. W każdym razie, jako że ustanawianie połączeń między wpisami stanowi operację przetwarzania danych, musi ono być zgodne z przepisami prawa krajowego transponującymi dyrektywę 95/46/WE lub konwencję 108.

Wnioski podkreślają, że istnienie połączeń nie może wpłynąć na prawa dostępu (w przeciwnym wypadku dałoby dostęp do danych, których przetwarzanie nie byłoby zgodne z prawodawstwem krajowym z pogwałceniem art. 6 dyrektywy).

EIOD podkreśla znaczenie rygorystycznej interpretacji art. 26 wniosku dotyczącego rozporządzenia i art. 46 wniosku dotyczącego decyzji: jedyną drogą zapewnienia tego jest wyjaśnienie, że organy niemające prawa dostępu do pewnych kategorii danych nie tylko nie mogą mieć dostępu do połączeń z wpisami z tych kategorii, ale nie powinny nawet być świadome istnienia tych połączeń. Wizualizacja połączeń nie może być możliwa w przypadku braku prawa dostępu do danych wchodzących w dane połączenie.

Ponadto EIOD pragnąłby być konsultowany co do środków technicznych gwarantujących spełnienie powyższego wymogu.

4.4. **Wpisy w celu odmowy wjazdu**

4.4.1. *Podstawy włączenia*

Wykorzystanie „wpisów dokonanych wobec obywateli państw trzecich w celu odmowy wjazdu" (art. 15 rozporządzenia) ma znaczący wpływ na swobody osoby: osoba, wobec której dokonano wpisu zgodnie z powyższym przepisem, nie ma wstępu na terytorium Schengen przez kilka lat. Jak dotąd tego rodzaju wpisu dokonano w stosunku do największej liczby osób. Biorąc pod uwagę konsekwencje tego wpisu oraz liczbę dotkniętych osób, należy podchodzić do koncepcji wpisu i jego realizacji z wielką ostrożnością. Choć uwaga ta jest również prawdziwa w odniesieniu do innych typów wpisów, EIOD poświęci osobny rozdział wpisom w celu odmowy wjazdu, gdyż stawiają one szczególne problemy jeżeli chodzi o podstawy ich włączenia.

Nowy wpis w celu odmowy wjazdu jest lepszy niż obecnie stosowany, ale też nie jest zupełnie satysfakcjonujący, jako że oparto go w dużym stopniu na instrumentach, które nie zostały jeszcze przyjęte, a nawet co do których nie złożono jeszcze wniosku.

Ulepszenia polegają na precyzyjniejszym opisie podstaw włączenia danych. Obecne sformułowanie konwencji z Schengen doprowadziło do znaczących różnic w liczbie osób, wobec których poszczególne państwa członkowskie dokonywały wpisu na mocy art. 96 konwencji. Wspólny organ nadzorczy Schengen przeprowadził szeroko zakrojone studium ([1]) tego zagadnienia i zalecił, by „politycy rozważyli ujednolicenie przyczyn tworzenia wpisu w poszczególnych państwach Schengen".

Art. 15 wniosku jest sformułowany bardziej szczegółowo, co należy zauważyć z zadowoleniem.

Ponadto art. 15 ust. 2 zawiera wykaz przypadków, w których nie można dokonać wpisów wobec pewnych osób, gdyż przebywają one na terytorium państwa członkowskiego legalnie, mając różny status. Chociaż można to wywnioskować z aktualnej konwencji z Schengen, w praktyce okazało się, że istnieją różnice w stosowaniu tego mechanizmu w poszczególnych państwach członkowskich. Z tego powodu z zadowoleniem przyjmuje się wyjaśnienie.

Przepis ten jest jednak także poddawany poważnej krytyce, gdyż został w dużej części oparty na tekście jak dotąd nieprzyjętym, mianowicie na dyrektywie „w sprawie powrotu".

Po przyjęciu wniosków dotyczących SIS II Komisja złożyła (1 września 2005 r.) wniosek dotyczący „dyrektywy w sprawie wspólnych norm i procedur dla państw członkowskich dotyczących powrotu nielegalnych imigrantów z państw trzecich", lecz dopóki nie ma wersji ostatecznej tego tekstu, nie może on być uważany za ważną podstawę wprowadzania danych do systemu. Stanowi to w szczególności pogwałcenie art. 8 europejskiej konwencji praw człowieka, gdyż naruszenie prywatności osób powinno być uzasadnione m.in. jasnym i dostępnym prawodawstwem.

Dlatego EIOD wzywa Komisję do wycofania tego przepisu lub przeformułowania go w taki sposób, aby był on oparty na istniejącym prawodawstwie; który umożliwiałby osobom dokładne poznanie środków, które właściwe organy mogą zastosować wobec nich.

4.4.2. *Dostęp do wpisów opartych na art. 15*

Art. 18 określa, które organy mają dostęp do tych wpisów i do jakich celów. Art. 18 ust. 1 i 2 określają, które organy mają dostęp do wpisów dokonanych w oparciu o dyrektywę w sprawie powrotu. Ma tutaj zastosowanie uwaga zamieszczona powyżej.

([1]) Sprawozdanie wspólnego organu nadzorczego Schengen dotyczące inspekcji stosowania wpisów na podstawie art. 96 w Systemie Informacyjnym Schengen, Bruksela, 20 czerwca 2005 r.

Art. 18 ust. 3 wniosku dotyczącego rozporządzenia umożliwia dostęp organom odpowiedzialnym za przyznawanie statusu uchodźcy, zgodnie z dyrektywą, co do której nie złożono jeszcze nawet wniosku. Z braku dostępnego tekstu EIOD musi powtórzyć uwagi przedstawione powyżej.

4.4.3. *Okres zatrzymywania wpisów opartych na art. 15*

Zgodnie z art. 20 wpis nie może być zatrzymywany dłużej niż okres odmowy wjazdu określony w decyzji (o usunięciu lub powrocie). Jest to spójne z zasadami ochrony danych. Ponadto wpis zostanie usunięty automatycznie po pięciu latach, o ile państwo członkowskie, które wpisało dane do SIS II, nie zadecyduje inaczej.

Odpowiedni nadzór na szczeblu krajowym powinien zapewnić niestosowanie nieuzasadnionego automatycznego przedłużania okresu zatrzymywania oraz usuwanie przez państwa członkowskie danych przed upływem pięciu lat, jeżeli okres odmowy wjazdu jest krótszy.

4.5. **Okresy zatrzymywania**

Chociaż zasada zatrzymywania danych pozostaje ta sama (ogólnie rzecz biorąc, wpis powinien zostać usunięty z SIS II zaraz po wykonaniu działania wymaganego wpisem), w rezultacie stosowania omawianych wniosków okres zatrzymywania wpisów ogólnie zostanie przedłużony.

Konwencja z Schengen przewiduje przegląd potrzeby ciągłego przechowywania danych nie później niż trzy lata po ich wprowadzeniu (lub po roku w przypadku danych wprowadzonych w celu niejawnego nadzoru). Nowe wnioski przewidują automatyczne usuwanie (z możliwością sprzeciwu ze strony państwa członkowskiego, które dokonało wpisu) po pięciu latach dla danych o imigracji, po dziesięciu latach dla danych o aresztowaniach, osobach poszukiwanych i wezwanych do stawienia się w związku z postępowaniem sądowym oraz po trzech latach dla danych o osobach, które mają zostać objęte nadzorem niejawnym.

Chociaż w zasadzie państwa członkowskie będą musiały usunąć dane, kiedy zrealizowany zostanie cel wpisu, powyższe dane oznaczają znaczące przedłużenie maksymalnego okresu zatrzymywania danych (w większości wypadków trzykrotne) bez żadnego uzasadnienia ze strony Komisji. W przypadku danych o imigracji można jedynie zgadywać, że pięcioletni okres jest związany z okresem zakazu wjazdu proponowanym w projekcie dyrektywy o powrocie. W pozostałych przypadkach EIOD nie jest świadomy żadnego uzasadnienia.

Potencjalny wpływ na osoby, których dotyczą wpisy w SIS, może mieć znaczące konsekwencje dla ich życia. Jest to szczególnie niepokojące w przypadku wpisów wobec osób, które mają zostać poddane nadzorowi niejawnemu lub szczególnym kontrolom, jako że wpisy te mogą być dokonywane na podstawie podejrzeń.

EIOD pragnąłby zapoznać się z poważnym uzasadnieniem przedłużenia okresów zatrzymywania danych. Jeżeli brak jest przekonywującego uzasadnienia, sugeruje ich skrócenie do obecnie stosowanego poziomu, zwłaszcza w przypadku wpisów do celów nadzoru niejawnego lub szczególnych kontroli.

4.6. **Dostęp przez organy odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów**

Podstawową kwestią jest wybór wielce wątpliwej podstawy prawnej. Komisja nie jest w stanie przekonywująco przedstawić zastosowania podstawy prawnej dotyczącej transportu i należącej do pierwszego filaru środka, który umożliwiłby dostęp do SIS organom administracyjnym w celu zapobiegania i zwalczania przestępczości (handlu kradzionymi pojazdami). Potrzeba silnego uzasadnienia i solidnej podstawy prawnej dla umożliwienia postępu do SIS II została szczegółowo opisana w pkt 4.2.2 niniejszej opinii.

EIOD odnosi się do dotyczących tego zagadnienia uwag wyrażonych przez wspólny organ nadzorczy Schengen w opinii w sprawie proponowanej podstawy prawnej dla SIS II. W szczególności należy zastosować się do propozycji wspólnego organu nadzorczego Schengen, by zmienić wniosek dotyczący decyzji w taki sposób, by włączyć do niej ten rodzaj dostępu.

5. ROLA KOMISJI I PAŃSTW CZŁONKOWSKICH

Jasny opis i określenie obowiązków w kontekście SIS II jest niezwykle ważne, nie tylko dla sprawnego funkcjonowania systemu, ale także z punktu widzenia nadzoru. Dystrybucja kompetencji nadzorczych będzie wynikać z opisu obowiązków, stąd potrzeba jak największej jasności.

5.1. **Rola Komisji**

EIOD z zadowoleniem przyjmuje rozdział III obydwu wniosków opisujący rolę i obowiązki Komisji w odniesieniu do SIS II („zarządzanie operacyjne"). Takie wyjaśnienia nie zostały ujęte we wniosku dotyczącym VIS. Mimo to wspomniany rozdział nie definiuje wyczerpująco roli Komisji. Jak określono w rozdziale 9 niniejszej opinii, Komisja ma również wkład we wdrażanie systemu i zarządzanie nim za pomocą procedury komitologii.

W kontekście ochrony danych Komisja odgrywa rolę uznaną już w systemach VIS i Eurodac, polegającą na odpowiedzialności za zarządzanie operacyjne. W połączeniu z jej znaczącą rolą w opracowaniu i utrzymywaniu systemu jest w zasadzie organem kontrolującym *sui generis*. Zgodnie z opinią EIOD na temat VIS, jest to rola o wiele bardziej istotna niż rola przetwarzającego, ale też bardziej ograniczona niż normalnego organu kontrolującego, gdyż Komisja nie ma dostępu do danych przetwarzanych w SIS II.

Jako że SIS II będzie oparty na skomplikowanych systemach, w części opartych na rozwijających się technologiach, EIOD naciska na wzmocnienie odpowiedzialności Komisji za utrzymanie i aktualizacje systemów z wykorzystaniem najlepszym dostępnych technologii w dziedzinie bezpieczeństwa i ochrony danych.

Należy w takim razie dodać w art. 12 wniosków, że Komisja powinna regularnie wnioskować o zastosowanie nowych technologii stanowiących najnowocześniejsze rozwiązania w tej dziedzinie, co podniesie poziom ochrony i bezpieczeństwa danych oraz ułatwi wykonywanie zadań organom krajowym mającym do nich dostęp.

5.2. **Rola państw członkowskich**

Sytuacja państw członkowskich nie jest jasna, jako że trudno jest się dowiedzieć, który(e) organ(-y) będzie(będą) organem(-ami) kontrolującym(-i).

We wnioskach opisano rolę Krajowego Biura SIS II (zapewniającego właściwym organom dostęp do SIS II) oraz organów SIRENE (zapewniających wymianę wszelkich informacji uzupełniających). Państwa członkowskie muszą także zapewnić funkcjonowanie i bezpieczeństwo ich „NS" (systemu krajowego). Nie jest jasne, czy ten ostatni obowiązek dotyczy któregokolwiek z powyższych organów. Tak czy inaczej, konieczne jest wyjaśnienie.

W kontekście ochrony danych Komisja i państwa członkowskie powinny być uważane za wspólne organy kontrolujące, z których każdy ma szczególne obowiązki. Uznanie tych dodatkowych zadań jest jedynym sposobem na uniknięcie pozostawienia któregoś obszaru działalności SIS II bez nadzoru.

6. **PRAWA OSÓB, KTÓRYCH DOTYCZĄ DANE**

6.1. **Informacje**

6.1.1. *Wniosek dotyczący rozporządzenia*

Art. 28 wniosku dotyczącego rozporządzenia przewiduje prawo osoby, której dotyczą dane, do informacji, w oparciu głównie o art. 10 dyrektywy 95/46. Jest to pozytywna zmiana w stosunku do obecnej sytuacji, gdyż konwencja nie przewiduje wyraźnie takiego prawa. Istnieje jednak możliwość wprowadzenia kilku ulepszeń w następujących punktach.

Do wykazu należałoby dodać pewne informacje, gdyż wpłynęłoby to na zapewnienie sprawiedliwego traktowania osób, których dotyczą dane ([1]). Informacje te powinny dotyczyć okresu zatrzymywania danych, prawa do złożenia odwołania lub zwrócenia się z wnioskiem o kontrolę decyzji o dokonaniu wpisu (w niektórych przypadkach zob. art. 15 ust. 3 wniosku dotyczącego rozporządzenia), możliwości uzyskania pomocy ze strony organu ochrony danych oraz istnienia środków odwoławczych.

We wniosku dotyczącym rozporządzenia nie wskazano terminu, w jakim powinna zostać przekazana informacja. Może to sprawić, że prawa osoby, której dotyczą dane, będą niemożliwe do wyegzekwowania. Aby prawa te były skuteczne, rozporządzenie powinno określać dokładny moment podania informacji w zależności od organu dokonującego wpisu.

Praktycznym rozwiązaniem byłoby przede wszystkim dodanie informacji o dokonaniu wpisu w decyzji uzasadniającej wpis: decyzji sądowej lub administracyjnej wynikającej z zagrożenia dla porządku publicznego (…) lub decyzji o powrocie lub nakazie wydalenia, któremu towarzyszy zakaz ponownego wjazdu. Powyższe należy włączyć do art. 28 rozporządzenia.

6.1.2. *Wniosek dotyczący decyzji*

Art. 50 decyzji stanowi, że informacji udziela się na wniosek osoby, której dotyczą dane, i że podaje się możliwe podstawy odmowy udzielenia takich informacji. Oczywiście zrozumiałe są ograniczenia tego prawa, biorąc pod uwagę charakter danych oraz kontekst, w jakim są przetwarzane.

Jednak prawo do informacji nie może być uzależnione od złożenia wniosku przez osobę, której dotyczą dane (raczej stanowiłoby to definicję wniosku o udzielenie dostępu). Można przyjąć, że potrzeba „zwracania się z wnioskiem" o informację jest uzasadniona przypadkami, w których osoby, której dotyczą dane, nie można poinformować, gdyż nie zdołano jej zlokalizować.

Kwestię tę można lepiej rozwiązać dodając wyjątek do prawa do informacji w przypadkach, gdy udzielenie informacji okazuje się niemożliwe lub wiąże się z nieproporcjonalnym wysiłkiem. Art. 50 decyzji powinien zostać odpowiednio zmieniony,

([1]) Podobna kwestia w opinii EIOD w sprawie ustanowienia Systemu Informacji Wizowej, pkt 3.10.1.

Rozwiązanie takie byłoby również spójne z zastosowaniem projektu decyzji ramowej w sprawie ochrony danych w trzecim filarze.

6.2. **Dostęp**

Obydwa wnioski, dotyczące rozporządzenia i decyzji, ustanawiają nieprzekraczalne terminy udzielania odpowiedzi na wnioski o udzielenie dostępu, co stanowi pozytywną zmianę. Jednak jako że procedura korzystania z prawa dostępu została zdefiniowana na szczeblu krajowym, należy się zastanowić, w jaki sposób terminy narzucone we wnioskach mogą współgrać z istniejącymi procedurami, szczególnie w przypadkach gdy państwa członkowskie określiły krótsze terminy odpowiedzi na wnioski o udzielenie dostępu. Należałoby wyjaśnić, że powinno się stosować terminy najkorzystniejsze dla osoby, której dotyczą dane.

6.2.1. *Wniosek dotyczący rozporządzenia*

Należy zauważyć, że ograniczenia prawa dostępu („odmawia się, jeżeli jest to konieczne dla wykonania zgodnego z prawem zadania w związku z wpisem lub dla ochrony praw i swobód stron trzecich"), obecnie istniejące w konwencji z Schengen, nie zostały przeniesione do wniosku dotyczącego rozporządzenia.

Jest to prawdopodobnie wynikiem stosowalności dyrektywy 95/46/WE, która przewiduje (w art. 13) możliwość wprowadzenia wyjątków w prawodawstwie krajowym. Tak czy inaczej należy wskazać, że zastosowanie art. 13 w prawodawstwie krajowym w celu ograniczenia prawa dostępu powinno zawsze być zgodne z art. 8 EKPC i mieć miejsce w szczególnych przypadkach.

6.2.2. *Wniosek dotyczący decyzji*

Wniosek dotyczący decyzji przejmuje ograniczenie prawa dostępu określone w konwencji z Schengen. Wniosek dotyczący decyzji ramowej zawiera w zasadzie te same ograniczenia prawa dostępu, więc przyjęcie tego instrumentu nie wniesie żadnej istotnej różnicy.

Ze względu na to, że w niektórych państwach członkowskich dostęp do danych wykorzystywanych przez organy ochrony porządku publicznego jest „niebezpośredni" (co oznacza, że dane są dostępne za pośrednictwem krajowego organu ochrony danych), przydatne byłoby zapewnienie obowiązku aktywnej współpracy w wykonywaniu prawa dostępu ze strony organów ochrony danych.

6.3. **Prawo do złożenia odwołania lub zwrócenia się z wnioskiem o kontrolę decyzji o dokonaniu wpisu**

Art. 15 ust. 3 rozporządzenia ustanawia prawo do złożenia odwołania lub zwrócenia się z wnioskiem do organu sądowego o kontrolę decyzji o dokonaniu wpisu, jeżeli decyzja taka została podjęta przez organ administracyjny. Jest to pozytywna zmiana w stosunku do obecnego brzmienia konwencji z Schengen.

Podkreśla to potrzebę pełnego i terminowego informowania osoby, której dotyczą dane, wspomnianego w pkt 6.1 powyżej: bez informowania zainteresowanej osoby to nowe prawo pozostanie w sferze teorii.

6.4. **Środki odwoławcze**

Art. 30 wniosku dotyczącego rozporządzenia i art. 52 wniosku dotyczącego decyzji przewidują prawo do wszczęcia postępowania lub wniesienia skargi przed sądami jakiegokolwiek państwa członkowskiego, jeżeli osoba, której dotyczą dane, otrzyma odmowę prawa dostępu lub prawa do korekty lub usunięcia danych jej dotyczących lub prawa do uzyskania informacji lub odszkodowania.

To sformułowanie („każda osoba na terytorium państwa członkowskiego") sugeruje, że powód musi znajdować się fizycznie na terytorium państwa w celu wszczęcia postępowania. To ograniczenie terytorialne jest nieuzasadnione i może uczynić prawo do wykorzystania środków odwoławczych nieskutecznym, gdyż w wielu przypadkach powód pragnie wszcząć postępowanie właśnie z powodu odmówienia mu wjazdu na terytorium Schengen. Ponadto, w tym co odnosi się do wniosku dotyczącego rozporządzenia, jako że dyrektywa stanowi *lex generalis*, należy wziąć pod uwagę jej art. 22. Stanowi on, że „każda osoba" ma prawo do zastosowania środka sądowego bez względu na miejsce jej zamieszkania. Wniosek dotyczący decyzji ramowej także nie zawiera ograniczenia terytorialnego. EIOD sugeruje usunięcie ograniczenia terytorialnego z art. 30 i 52.

7. **NADZÓR**

7.1. **Uwaga wstępna: podział obowiązków**

Wnioski przewidują podział zadań związanych z nadzorem pomiędzy krajowe organy nadzorcze [1] a EIOD, w odpowiednim dla każdego z nich zakresie. Jest to zgodne z reprezentowanym we wnioskach podejściem do prawa stosowanego i odpowiedzialności za funkcjonowanie i korzystanie z SIS II oraz z potrzebą istnienia skutecznego nadzoru.

Z tego powodu EIOD z zadowoleniem przyjmuje to podejście wyrażone w art. 31 wniosku dotyczącego rozporządzenia i art. 53 wniosku dotyczącego decyzji. Jednak, dla lepszego zrozumienia oraz wyjaśnienia odpowiednich zadań, EIOD proponuje rozbicie każdego z artykułów na kilka oddzielnych przepisów, z których każdy byłby poświęcony pewnemu poziomowi nadzoru, na wzór wniosku dotyczącego VIS.

[1] Organy nadzorcze Europolu i Eurojustu także uczestniczą w tym procesie, lecz w mniejszym zakresie.

7.2. **Nadzór sprawowany przez krajowe organy ochrony danych**

Zgodnie z art. 31 wniosku dotyczącego rozporządzenia i art. 53 wniosku dotyczącego decyzji każde państwo członkowskie musi zapewnić monitorowanie zgodności z prawem przetwarzania danych osobowych zawartych w SIS II przez niezależny organ.

Art. 53 wniosku dotyczącego decyzji dodaje prawo osoby do zwrócenia się do organu nadzorującego o sprawdzenie zgodności z prawem przetwarzania danych jej dotyczących. We wniosku dotyczącym rozporządzenia nie znalazł się podobny zapis, gdyż dyrektywa stosuje się jako *lex generalis*. Z tego powodu należy brać pod uwagę, że krajowe organy ochrony danych mogą realizować w odniesieniu do SIS II wszystkie kompetencje przyznane im na mocy art. 28 dyrektywy 95/46/WE, w tym sprawdzanie zgodności z prawem przetwarzania danych. Art. 31 ust. 1 rozporządzenia zawiera wyjaśnienia zadań tych organów, ale nie może stanowić ograniczenia ich uprawnień. Uznanie wspomnianych kompetencji powinno zostać wyjaśnione w tekście wniosku dotyczącego rozporządzenia.

Odnośnie do wniosku dotyczącego decyzji, uznaje on większe obowiązki krajowych organów nadzorczych, gdyż *lex generalis* różni się w tym przypadku. Jednak sytuacja, w której organy nadzorcze miałyby różne zadania i kompetencje w zależności od kategorii przetwarzanych danych nie jest właściwa i zarządzanie nią w praktyce sprawiałoby wiele problemów. Z tego powodu należy uniknąć takiej sytuacji poprzez przyznanie wspomnianym organom tych samych uprawnień w samym tekście wniosku dotyczącego decyzji lub poprzez odniesienie do innego *lex generalis* (mianowicie decyzji ramowej w sprawie ochrony danych w trzecim filarze), co zwiększy kompetencje organów ochrony danych.

7.3. **Nadzór sprawowany przez EIOD**

EIOD monitoruje przeprowadzanie przez Komisję działań związanych z przetwarzaniem danych zgodnie z omawianymi wnioskami. Podobnie EIOD powinien być w stanie wykorzystywać wszystkie kompetencje przyznane mu rozporządzeniem 45/2001, uwzględniając jednak ograniczone uprawnienia Komisji w odniesieniu do samych danych.

Właściwym jest dodać, że zgodnie z art. 46 lit f) rozporządzenia 45/2001 EIOD „współpracuje z krajowymi organami nadzoru w stopniu koniecznym dla wykonywania ich obowiązków". Współpraca z państwami członkowskimi w ramach nadzoru nad SIS II nie wynika tylko z omawianych wniosków, lecz także z rozporządzenia 45/2001.

7.4. **Wspólny nadzór**

Wnioski uznają również potrzebę koordynacji działań nadzorczych różnych zaangażowanych w nie organów. Art. 31 wniosku dotyczącego rozporządzenia i art. 53 wniosku dotyczącego decyzji stanowią, że „krajowe organy nadzorcze i Europejski Pełnomocnik ds. Ochrony Danych aktywnie ze sobą współpracują. Europejski Pełnomocnik ds. Ochrony Danych zwołuje w tym celu posiedzenie przynajmniej raz do roku."

EIOD z zadowoleniem przyjmuje ten wniosek, który zawiera w zasadzie wszystkie elementy niezbędne do ustanowienia współpracy — która jest kwestią fundamentalną — pomiędzy organami odpowiedzialnymi za nadzór na szczeblu krajowym i europejskim. Należy podkreślić, że we wnioskach przewidziano posiedzenia przynajmniej raz w roku, co należy uważać za częstotliwość minimalną.

Te przepisy (art. 31 wniosku dotyczącego rozporządzenia i art. 53 wniosku dotyczącego decyzji) mogłyby jednak zostać ulepszone dzięki włączeniu wyjaśnień dotyczących szczegółów takiej koordynacji. Do kompetencji istniejącego wspólnego organu nadzorczego należy analiza trudności w interpretacji lub stosowaniu konwencji, badanie problemów, które mogą występować podczas realizacji niezależnego nadzoru lub prawa dostępu, oraz przygotowywanie zharmonizowanych wniosków dotyczących wspólnych rozwiązań istniejących problemów.

Nowe wnioski nie mogą prowadzić do rozmycia obecnego zakresu wspólnego nadzoru. Jeżeli jasnym jest, że organy ochrony danych mogą realizować w odniesieniu do SIS II wszystkie kompetencje, które przyznaje im dyrektywa, współpraca pomiędzy tymi organami może odnosić się do ogólnych aspektów nadzoru nad SIS II, w tym do zadań istniejącego wspólnego organu nadzorczego, o którym mowa w art. 115 konwencji z Schengen.

Mimo to, by uczynić to jednoznacznym, należałoby potwierdzić to wyraźnie w tekstach wniosków.

8. **BEZPIECZEŃSTWO**

Zarządzanie optymalnym poziomem bezpieczeństwa dla SIS II i poszanowanie tego poziomu stanowi podstawowy wymóg zapewniający odpowiednią ochronę danych osobowych przechowywanych w bazie danych. W celu osiągnięcia tego satysfakcjonującego poziomu ochrony należy wdrożyć odpowiednie zabezpieczenia, dzięki którym będzie można zarządzać potencjalnym ryzykiem związanym z infrastrukturą systemu i z osobami go obsługującymi. Temat ten jest poruszany w różnych częściach wniosku i wymaga wprowadzenia pewnych ulepszeń.

Art. 10 i 13 wniosku zawierają różne środki odnoszące się do bezpieczeństwa danych i wyszczególniają rodzaje nadużyć, którym należy zapobiegać. EIOD z zadowoleniem przyjmuje przepisy dotyczące systematycznej (auto)kontroli środków bezpieczeństwa zawarte w tych artykułach.

Art. 59 wniosku dotyczącego decyzji i art. 34 wniosku dotyczącego rozporządzenia, które przewidują monitorowanie i ocenę nie powinny dotyczyć wyłącznie aspektów takich jak wydajność, opłacalność i jakość usług, ale również zgodności z wymogami stawianymi przez prawo, zwłaszcza w dziedzinie ochrony danych. EIOD zaleca zatem rozszerzenie zakresu tych artykułów o monitorowanie zgodności z prawem przetwarzania danych oraz sprawozdań na ten temat.

Ponadto, w uzupełnieniu do art. 10 ust. 1 lit. f) lub art. 18 wniosku dotyczącego decyzji oraz art. 17 wniosku dotyczącego rozporządzenia dotyczących personelu upoważnionego do dostępu do danych, należy dodać, że państwa członkowskie (oraz Europol i Eurojust) powinny zapewnić dostępność dokładnych profilów użytkowników (które należy przechowywać do dyspozycji krajowych organów nadzorczych w celu przeprowadzania kontroli). Poza wspomnianymi profilami użytkowników, Państwa Członkowskie muszą również opracować i stale uaktualniać kompletny spis tożsamości użytkowników. Powyższe ma zastosowanie *mutatis mutandis* do Komisji.

Powyższe środki bezpieczeństwa są uzupełniane poprzez monitorowanie i zabezpieczenia organizacyjne. Art. 14 wniosków opisuje warunki, w jakich należy przechowywać rejestry wszystkich operacji przetwarzania danych oraz cele takiego przechowywania. Rejestry te powinny być przechowywane nie tylko do celu monitorowania ochrony danych i zapewniania ich bezpieczeństwa, ale również dla przeprowadzania regularnej (auto)kontroli SIS II wymaganej art. 10. Sprawozdania z autokontroli przyczynią się do skutecznego wykonywania zadań organów nadzorczych, które będą w stanie określić najsłabsze punkty i skupić się na nich podczas przeprowadzanych przez nie kontroli.

Jak powiedziano wcześniej w niniejszej opinii, mnożenie punktów dostępu do systemu powinno być należycie uzasadnione, gdyż automatycznie zwiększa ryzyko nadużyć. Art. 4 ust. 1 lit. b) wniosków powinien więc zawierać wymóg szczegółowego uzasadnienia potrzeby ustanowienia drugiego punktu dostępu.

Wnioski nie wyjaśniają dostatecznie potrzeby tworzenia kopii krajowych systemu centralnego i wzbudzają poważne obawy co do całościowego poziomu ryzyka i bezpieczeństwa systemu, ponieważ:

— mnożenie kopii zwiększa ryzyko nadużyć (szczególnie biorąc pod uwagę wprowadzanie nowych danych, takich jak dane biometryczne);

— dane zawarte w tych kopiach nie są wystarczająco dobrze zdefiniowane;

— zawarte w art. 9 wymogi dotyczące dokładności, jakości i dostępności stanowią wielkie wyzwanie techniczne, tym samym zwiększając koszty w zależności od stanu zaawansowania dostępnej technologii;

— nadzorowanie tych kopii przez organy krajowe będzie wymagało dodatkowych zasobów ludzkich i finansowych, które mogą nie być ciągle dostępne.

Mając na uwadze związane z nią ryzyko, EIOD nie jest przekonany co do konieczności (uwzględniając dostępne technologie) ani wartości dodanej stosowania kopii krajowych. Zaleca usunięcie możliwości stosowania przez państwa członkowskie kopii krajowych.

Jeżeli jednak kopie krajowe mają zostać utworzone, EIOD przypomina, że musi zostać zastosowana zasada ścisłego ograniczenia celu do wykorzystania w obrębie kraju. Ponadto kopia krajowa nie może być przeszukiwana w jakikolwiek inny sposób niż centralna baza danych.

Zgodność z prawem operacji przetwarzania danych osobowych jest oparta na ścisłym poszanowaniu bezpieczeństwa i integralności danych. EIOD będzie skuteczniej monitorował te operacje, o ile umożliwi mu się monitorowanie nie tylko bezpieczeństwa danych, lecz także ich integralności poprzez analizę dostępnych rejestrów. Z tego powodu jest konieczne dodanie „integralności danych" do art. 14 ust. 6.

9. **KOMITOLOGIA**

Wnioski przewidują zastosowanie procedury komitologii w kilku przypadkach, gdy wymagane są decyzje techniczne dotyczące wdrożenia SIS II lub zarządzania nim. Jak przedstawiono w opinii dotyczącej VIS z podobnych powodów, decyzje te będą miały znaczący wpływ na właściwe stosowanie zasad celowości i proporcjonalności.

EIOD radzi, by decyzje mające znaczący wpływ na zagadnienia ochrony danych, jak na przykład dostęp do danych i ich wprowadzanie, wymiana informacji uzupełniających, jakość danych i kompatybilność wpisów, zgodność techniczna kopii krajowych itd. były podejmowane na podstawie rozporządzenia lub decyzji, najlepiej z zastosowaniem procedury współdecyzji ([1]).

([1]) Analogiczna kwestia została omówiona w opinii EIOD w sprawie Systemu Informacji Wizowej, pkt 3.12, oraz w opinii EIOD na temat wniosku dotyczącego dyrektywy w sprawie zatrzymywania danych przetwarzanych w związku ze świadczeniem publicznie dostępnych usług łączności elektronicznej wydanej dnia 26 września 2005 r., pkt 60.

We wszystkich innych kwestiach mających wpływ na ochronę danych, EIOD powinien mieć możliwość udzielania rad w sprawie wyborów dokonywanych przez te komitety.

Rola doradcza EIOD powinna zostać ujęta w art. 60-61 i art. 35 rozporządzenia.

W szczególnym przypadku zasad technicznych dotyczących połączeń między wpisami (art. 26 rozporządzenia i art. 46 decyzji) niezbędne jest wyjaśnienie konieczności zastosowanie innego rodzaju procedury komitologii (procedura doradcza w decyzji i procedura regulacyjna w rozporządzeniu).

10. **INTEROPERACYJNOŚĆ**

Z powodu braku komunikatu Komisji dotyczącego interoperacyjności tworzonych w obrębie UE systemów trudno jest właściwie ocenić wartość dodaną przewidywanych, lecz jeszcze nie zdefiniowanych synergii.

W tym kontekście EIOD chciałby również odwołać się do Deklaracji Rady z dnia 25 marca 2004 r. w sprawie zwalczania terroryzmu, w której Komisja jest proszona o przedstawienie wniosków mających za cel zwiększenie interoperacyjności i współdziałania pomiędzy systemami informacyjnymi (SIS, VIS i Eurodac). Chciałby również odwołać się do toczącej się dyskusji zajmującej się kwestią, któremu organowi należy powierzyć w przyszłości zarządzanie różnymi systemami o dużym zasięgu (patrz również pkt 3.8 niniejszej opinii).

EIOD stwierdził uprzednio w opinii w sprawie Systemu Informacji Wizowej, że interoperacyjność stanowi krytyczny i podstawowy wymóg dla skuteczności wielkoskalowych systemów teleinformatycznych, takich jak SIS II. Daje ona możliwość konsekwentnego zmniejszenia całkowitych kosztów i uniknięcia redundancji wśród heterogenicznych elementów składowych.

— Interoperacyjność może również przyczynić się do utrzymania wysokiego poziomu bezpieczeństwa na terytorium pozbawionym kontroli na granicach wewnętrznych pomiędzy państwami członkowskimi poprzez wdrożenie tych samych norm proceduralnych dotyczących wszystkich jej elementów składowych. Jednakże istotne jest wprowadzenie rozróżnienia pomiędzy dwoma poziomami interoperacyjności:

  — wysoce pożądana jest interoperacyjność pomiędzy państwami członkowskimi UE; w rzeczy samej wpisy dokonane przez organy jednego z państw członkowskich muszą być interoperacyjne z wpisami dokananymi przez organy innych państw członkowskich,

  — natomiast interoperacyjność pomiędzy systemami utworzonymi do innych celów lub z systemami państw trzecich budzi dużo większe wątpliwości.

Wśród dostępnych zabezpieczeń wykorzystywanych do ograniczenia celu systemu i zapobieżenia „zakłóceniom działania", znajduje się również możliwość wykorzystania różnych standardów technicznych. Ponadto każda forma interakcji pomiędzy dwoma różnymi systemami powinna być rzetelnie udokumentowana. Interoperacyjność nigdy nie powinna prowadzić do sytuacji, w której organ nie upoważniony do dostępu lub wykorzystania pewnych danych mógłby uzyskać dostęp poprzez inny system. Jak można wywnioskować z lektury wniosków, wydaje się, że na przykład system automatycznej identyfikacji odcisków palców (AFIS) nie będzie wdrożony w pierwszych latach działania SIS II; włączono jedynie odniesienie do przyszłej wyszukiwarki biometrycznej. Jeżeli przewiduje się scenariusz, w którym ma zastosowanie AFIS lub inne systemy UE, należy to jasno udokumentować i zastosować konieczne zabezpieczenia dla tego rodzaju synergii.

EIOD chciałby ponownie podkreślić, że wdrażanie interoperacyjności systemów nie może prowadzić do naruszenia zasady ograniczonego celu, oraz zaznacza, że każdy wniosek dotyczący tej kwestii powinien być mu przekazywany.

11. **STRESZCZENIE WNIOSKÓW**

11.1. **Punkty ogólne**

1. EIOD z zadowoleniem przyjmuje pozytywne aspekty omawianych wniosków, które w pewnych miejscach oznaczają poprawę w stosunku do obecnej sytuacji. Uznaje, że przepisy dotyczące ochrony danych, ogólnie rzecz biorąc, zostały przygotowane ze znaczną starannością.

2. EIOD podkreśla, że nowy system prawny, niezależnie od jego złożoności, powinien:

   — zapewnić wysoki poziom ochrony danych,

   — być przewidywalny zarówno dla obywateli, jak i dla organów wspólnie korzystających z danych,

   — stosować się w sposób spójny w różnych kontekstach (pierwszy lub trzeci filar).

3. Ponadto wprowadzenie do SIS II nowych elementów, zwiększające możliwy wpływ systemu na życie osób, powinno łączyć się z bardziej rygorystycznymi zabezpieczeniami opisanymi w niniejszej opinii. W szczególności

— nie można udzielać dostępu do SIS II nowym organom bez wyczerpującego uzasadnienia; dostęp powinien być jak najbardziej ograniczony, zarówno w odniesieniu do dostępnych danych, jak i uprawnionych do niego osób;

— połączenia między wpisami nie mogą nigdy prowadzić, nawet pośrednio, do zmiany prawa dostępu;

— dotąd nieprzyjęte akty prawne nie mogą być uznane za ważne podstawy dokonywania wpisów w SIS II (wpisy do celów odmowy wjazdu);

— podstawa prawna dostępu do danych przez organy odpowiedzialne za wydawanie dowodów rejestracyjnych pojazdów powinna zostać poddana ponownej refleksji, gdyż jej podstawową intencją jest zwalczanie przestępczości;

— EIOD uznaje, że wykorzystanie danych biometrycznych może poprawić wydajność systemu i pomóc ofiarom kradzieży tożsamości. Wpływ włączenia danych biometrycznych nie wydaje się jednak wystarczająco przemyślany, zaś wiarygodność tych danych wydaje się przesadzona.

11.2. **Uwagi szczegółowe**

1. EIOD z zadowoleniem przyjmuje uznanie przez Komisję, że rozporządzenie 45/2001 ma zastosowanie do wszystkich operacji przetwarzania danych w SIS II przeprowadzanych przez Komisję, gdyż przyczyni się to do zapewnienia spójnego i jednolitego stosowania zasad dotyczących ochrony podstawowych praw i swobód osób w odniesieniu do przetwarzania danych osobowych.

2. W celu zapewnienia ścisłego ograniczenia celu na szczeblu krajowym EIOD zaleca wprowadzenie do wniosków dotyczących SIS II (mianowicie do art. 21 wniosku dotyczącego rozporządzenia oraz art. 40 wniosku dotyczącego decyzji) przepisu o tym samym skutku co obecny art. 102 ust. 4 konwencji z Schengen, ograniczający państwom członkowskim możliwość wykorzystywania danych nieprzewidzianych w tekstach dotyczących SIS II.

3. Przyznając jakiemukolwiek organowi dostęp do SIS II należy stosować ściśle określone warunki:

— dostęp musi być spójny z ogólnym celem SIS II oraz zgodny z jego podstawą prawną;

— należy dowieść potrzeby dostępu do danych zawartych w SIS II;

— sposób wykorzystania danych musi zostać jasno zdefiniowany, wraz ze wszystkimi ograniczeniami;

— warunki dostępu muszą być jasno zdefiniowane i ograniczone; w szczególności należy sporządzić aktualizowaną listę osób mających prawo dostępu do SIS II, także w odniesieniu do Europolu i Eurojustu;

— fakt, że organy te mają dostęp do danych zawartych w SIS II nie może stanowić podstawy do wpisywania lub przechowywania danych w systemie, jeżeli nie są one przydatne dla wpisu, którego część stanowią;

— okres zatrzymywania danych nie może zostać przedłużony, jeżeli nie jest to konieczne do celów, dla których dokonano wpisu.

4. W szczególnych przypadkach Europolu i Eurojustu EIOD wzywa Komisję do ścisłego zdefiniowania zadań, których wykonywanie usprawiedliwiałoby ich dostęp do danych. Dostęp Europolu i Eurojustu do danych powinien ponadto zostać ograniczony do danych dotyczących osób, których nazwisko już znajduje się w ich aktach. Sugeruje się również przyznanie Europolowi i Eurojustowi tylko jednego punktu dostępu.

5. Odnośnie wpisów w celu odmowy wjazdu, przepisy oparte na dotychczas nieprzyjętych aktach prawnych powinny zostać wycofane lub przeformułowane w taki sposób — oparty na istniejącym prawodawstwie — który umożliwi zainteresowanym osobom dokładne poznanie środków, które właściwe organy mogą zastosować wobec nich.

6. Okresy zatrzymywania danych zostały przedłużone bez żadnego istotnego uzasadnienia. Jeżeli brak jest przekonywującego uzasadnienia, okresy te powinny zostać skrócone do obecnie stosowanego poziomu, zwłaszcza w przypadku wpisów do celów nadzoru niejawnego lub szczególnych kontroli.

7. Rola Komisji została zdefiniowana jako odpowiedzialność za zarządzanie operacyjne. W połączeniu z jej znaczącą rolą w opracowaniu i utrzymywaniu systemu jest w zasadzie organem kontrolującym *sui generis*. Jest to rola o wiele bardziej istotna niż rola przetwarzającego, ale też bardziej ograniczona niż normalnego organu kontrolującego, gdyż Komisja nie ma dostępu do danych przetwarzanych w SIS II.

   Odnośnie do wykonywania tej roli należy dodać w art. 12 obydwu wniosków, że Komisja powinna regularnie wnioskować o zastosowanie nowych technologii stanowiących najnowocześniejsze rozwiązania w tej dziedzinie, co podniesie poziom ochrony i bezpieczeństwa danych.

8. W odniesieniu do roli państw członkowskich konieczne jest wyjaśnienie funkcjonowania organów jako organów kontrolujących.

9. W odniesieniu do informowania osób, których dane dotyczą:

   — we wniosku dotyczącym rozporządzenia należy dodać do wykazu pewne informacje: okres zatrzymywania danych, istnienie prawa do złożenia odwołania lub zwrócenia się z wnioskiem o kontrolę decyzji o dokonaniu wpisu, możliwość uzyskania pomocy od organu ochrony danych oraz istnienie środków odwoławczych.

     Ponadto, w odniesieniu do terminu, w jakim powinna zostać przekazana informacja, przede wszystkim obowiązek podania informacji o dokonaniu wpisu w decyzji uzasadniającej wpis.

   — we wniosku dotyczącym decyzji należy wprowadzić zmianę do art. 50, by nie uzależniać prawa do informacji od złożenia wniosku przez osobę, której dotyczą dane.

10. Odnośnie do terminów odpowiedzi na wniosek o przyznanie dostępu, wskazane jest ustalenie tych terminów w omawianych wnioskach. Gdy prawodawstwo krajowe również ustanawia terminy, należałoby wyjaśnić, że powinno się stosować terminy najkorzystniejsze dla osoby, której dotyczą dane.

    Ponadto byłoby wskazane zapewnienie obowiązku aktywnej współpracy w wykonywaniu prawa do dostępu ze strony organów ochrony danych.

11. Odnośnie do prawa do środków odwoławczych, EIOD sugeruje zniesienie ograniczenia terytorialnego w art. 30 i art. 52.

12. Odnośnie do uprawnień krajowych organów ochrony danych:

    — w rozporządzeniu: należy uwzględnić, że mogą one realizować w odniesieniu do SIS II wszystkie kompetencje przyznane im na mocy art. 28 dyrektywy 95/46/WE; powinno to zostać wyjaśnione w tekście wniosku dotyczącego rozporządzenia.

    — we wniosku dotyczącym decyzji: organom nadzorczym należy przyznać te same uprawnienia, które przewidziano w rozporządzeniu/dyrektywie.

13. Odnośnie do kompetencji EIOD: EIOD powinien być w stanie wykorzystywać wszystkie kompetencje przyznane mu rozporządzeniem 45/2001, uwzględniając jednak ograniczone uprawnienia Komisji w odniesieniu do samych danych.

14. Odnośnie do koordynacji nadzoru: wnioski uznają również potrzebę koordynacji działań nadzorczych różnych zaangażowanych w nie organów. EIOD z zadowoleniem przyjmuje fakt, że wnioski zawierają w zasadzie wszystkie elementy niezbędne do ustanowienia współpracy pomiędzy organami odpowiedzialnymi za nadzór na szczeblu krajowym i europejskim. Te przepisy (art. 31 wniosku dotyczącego rozporządzenia i art. 53 wniosku dotyczącego decyzji) mogłyby jednak zostać ulepszone dzięki włączeniu wyjaśnień dotyczących szczegółów takiej koordynacji.

15. Art. 10 i 13 wniosku zawierają różne środki bezpieczeństwa danych; wskazane jest włączenie przepisów dotyczących systematycznej (auto) kontroli środków bezpieczeństwa.

    — Art. 59 wniosku dotyczącego decyzji i art. 34 wniosku dotyczącego rozporządzenia, które przewidują monitorowanie i ocenę nie powinny dotyczyć wyłącznie aspektów takich jak wydajność, opłacalność i jakość usług, ale również zgodności z wymogami stawianymi przez prawo, zwłaszcza w dziedzinie ochrony danych. Przepisy te powinny zostać odpowiednio zmienione.

    — Ponadto, w uzupełnieniu do art. 10 ust. 1 lit. f) lub art. 18 wniosku dotyczącego decyzji oraz art. 17 wniosku dotyczącego rozporządzenia należy dodać, że państwa członkowskie, Europol i Eurojust powinny zapewnić dostępność dokładnych profilów użytkowników (które należy przechowywać do dyspozycji krajowych organów nadzorczych w celu przeprowadzania kontroli). Poza wspomnianymi profilami użytkowników, państwa członkowskie muszą również opracować i stale uaktualniać kompletny spis tożsamości użytkowników. Powyższe ma zastosowanie do Komisji.

    — Zgodność z prawem operacji przetwarzania danych osobowych jest oparta na ścisłym poszanowaniu bezpieczeństwa i integralności danych. EIOD powinien mieć możliwość monitorowania nie tylko bezpieczeństwa danych, lecz także ich integralności poprzez analizę dostępnych rejestrów. Z tego powodu konieczne jest dodanie „integralności danych" do art. 14 ust. 6.

16. Stosowanie kopii krajowych może się wiązać z dodatkowym ryzykiem. EIOD nie jest przekonany co do konieczności (uwzględniając dostępne technologie) ani wartości dodanej stosowania kopii krajowych. Zaleca unikanie lub co najmniej znaczne ograniczenie możliwości wykorzystywania przez państwa członkowskie kopii krajowych. Jeżeli jednak kopie krajowe mają zostać utworzone, musi zostać zastosowana zasada ścisłego ograniczenia celu do wykorzystania w obrębie kraju. Ponadto kopia krajowa nie może być przeszukiwana w jakikolwiek inny sposób niż centralna baza danych.

17. Odnośnie do komitologii: decyzje mające znaczący wpływ na ochronę danych powinny zostać uregulowane, jeśli jest to możliwe, rozporządzeniem, najlepiej z wykorzystaniem procedury współdecyzji. Gdy wykorzystuje się procedurę komitologii, rola doradcza EIOD powinna zostać ujęta w art. 60-61 decyzji i art. 35 rozporządzenia.

18. Interoperacyjność systemów nie może być wdrażana z pogwałceniem zasady ograniczonego celu, zaś każdy dotyczący tej kwestii wniosek powinien zostać przedłożony EIOD.

Sporządzono w Brukseli dnia 19 października 2005 r.

Peter HUSTINX

Europejski Inspektor Ochrony Danych