Opinia Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniającego decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399 i rozporządzenie (UE) 2017/2226”

[COM(2017) 793 final – 2017/0351(COD)]

„Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja)”

[COM(2017) 794 final – 2017/0352(COD)]

(2018/C 283/07)

Sprawozdawczyni: **Laure BATUT**

Wniosek o konsultację	Komisja Europejska, 18.1.2018
	Parlament Europejski, 28.2.2018
Podstawa prawna	Artykuł 304 Traktatu o funkcjonowaniu Unii Europejskiej
Sekcja odpowiedzialna	Sekcja Zatrudnienia, Spraw Społecznych i Obywatelstwa
Data przyjęcia przez sekcję	25.4.2018
Data przyjęcia na sesji plenarnej	23.5.2018
Sesja plenarna nr	535
Wynik głosowania	160/3/2
(za/przeciw/wstrzymało się)	

1. **Wnioski i zalecenia**

1.1. EKES za pożyteczną i właściwą uważa propozycję Komisji Europejskiej mającą na celu poprawę interoperacyjności systemów informacyjnych UE dotyczących granic i polityki wizowej oraz współpracy policyjnej i sądowej, azylu i migracji.

1.2. EKES uważa, że interoperacyjność ta musi być strategicznym celem UE, aby pozostała ona nadal otwartą przestrzenią z gwarancją praw podstawowych i mobilności. UE i państwa członkowskie mają obowiązek chronić życie i bezpieczeństwo wszystkich ludzi; zasada *non-refoulement* powinna być w pełni przestrzegana.

1.3. Środki na rzecz interoperacyjności będą lepiej rozumiane, jeżeli:

— zapewnią w polityce migracyjnej UE równowagę między wolnością a bezpieczeństwem w otwartej Europie, z poszanowaniem rozdziału władzy,

— zagwarantują osobom zainteresowanym poszanowanie przysługujących im praw podstawowych, w szczególności bezpieczeństwo danych osobowych i prywatności, prawo dostępu do danych osobowych, ich sprostowania i usuwania w rozsądnym terminie, w ramach dostępnych procedur,

— potwierdzą, w tym we wszystkich aktach wykonawczych, wymóg uwzględnienia ochrony prywatności już w fazie projektowania („privacy by design”),

— nie stworzą nowych przeszkód dla normalnego ruchu podróżnych i towarów.

1.4. EKES wzywa do opracowania takich procedur i gwarancji w odniesieniu do wykorzystania danych do celów egzekwowania prawa, które:

— będą przewidywać stosowanie w tym obszarze przepisów europejskich zapewniających najwyższy poziom ochrony (ogólne rozporządzenie o ochronie danych),

— pozwolą przyspieszyć wskazanie państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej,

— zagwarantują osobom zainteresowanym prawo do dwuinstancyjnego postępowania;

— zagwarantują osobom małoletnim, w szczególności osobom małoletnim bez opieki – niezależnie od tego, czy mają one uregulowany status, czy są prześladowane lub czy ciążą na nich zarzuty karne – prawo uzyskania wizy, prawo do ochrony i integracji oraz do korzystania z prawa do bycia zapomnianym w czasie krótszym niż w przypadku osób pełnoletnich.

1.5. EKES uważa, że obecna podstawa prawna systemów informacyjnych powinna zostać wzmocniona i powinna uwzględniać możliwość modernizacji systemów gromadzenia danych. EKES zaleca, aby:

— zwiększyć bezpieczeństwo istniejących baz danych oraz powiązanych kanałów komunikacji,

— zapewnić ocenę wpływu zwiększenia kontroli wstępnej na zarządzanie ryzykiem,

— zapewnić kontrolę i stałą ocenę architektury systemów przez organy ochrony danych (EIOD). Wymaga to nałożenia na podmioty odpowiedzialne wymogu przedkładania organom decyzyjnym i Komisji co roku informacji na temat bezpieczeństwa elementów interoperacyjności oraz co dwa lata informacji na temat wpływu stosowanych środków na prawa podstawowe.

1.6. EKES uważa, że projekt powinien być realizowany przez kompetentny personel i sugeruje:

— programy gruntownego szkolenia dla odpowiednich organów i urzędników eu-LISA,

— wnikliwe sprawdzanie kwalifikacji urzędników tej agencji i kandydatów do niej.

1.7. EKES wyraża zaniepokojenie co do finansowania nowego systemu. Monitorowanie planowania będzie miało kluczowe znaczenie dla uniknięcia przekroczenia budżetu i dla prowadzenia projektu aż do jego zakończenia, czyli do 2029 r.

1.8. EKES zaleca, aby obywatele byli informowani o postępach w realizacji projektu aż do jego zakończenia i by osobom podlegającym kontrolom udzielano informacji wyjaśniających na temat tych kontroli. Uważa, że należy przewidzieć możliwość zatrzymania realizacji, jeżeli wolność i podstawowe prawa zostałyby zagrożone przez niewłaściwe wykorzystanie systemu.

2. **Wprowadzenie**

2.1. W 2017 r., gdy sytuację międzynarodową uważano za niestabilną zarówno pod względem geopolitycznym, jak i bezpieczeństwa wewnętrznego państw członkowskich, Rada zwracała się kilkakrotnie do Komisji o wdrożenie środków umożliwiających znalezienie śladów osób uznawanych za „stanowiące zagrożenie", które były już notowane w jednym z państw członkowskich. Uzyskanie informacji o przekroczeniu przez te osoby granic, ich podróżach i trasach poruszania się po Europie mogłoby mieć kluczowe znaczenie dla bezpieczeństwa w Unii.

2.2. W rezolucji z dnia 6 lipca 2016 r. Parlament zaapelował do Komisji Europejskiej o zapewnienie niezbędnych gwarancji w zakresie ochrony danych.

2.3. Omawiane wnioski wpisują się w cel „utrzymania i wzmocnienia strefy Schengen" ([1]). Unia posiada już wiele przepisów i elektronicznych serwisów informacyjnych w dziedzinach związanych z kontrolą przekraczania granic przez osoby i towary.

2.4. Dla przypomnienia:

— **SIS: system informacyjny Schengen** – jeden z najstarszych mechanizmów, poddany przeglądowi, służy do obsługi szerokiego zakresu ostrzeżeń dotyczących osób i towarów.

([1]) COM(2017) 570 final.

— **Eurodac: europejski zautomatyzowany system identyfikacji odcisków palców** osób ubiegających się o azyl i obywateli państw trzecich o nieuregulowanym statusie na granicach i w państwach członkowskich, służący również do określania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku (CESE 2016-02981, sprawozdawca: Moreno Díaz ([2])).

— **VIS: wizowy system informacyjny** (kodeks wizowy), który służy do obsługi wiz krótkoterminowych (CESE 2014-02932, sprawozdawcy: Pezzini i Pariza Castaños ([3])).

— **EES: system wjazdu/wyjazdu**, obecnie oczekujący na decyzję, którego zadaniem miałaby być elektroniczna obsługa danych zawartych w paszportach i danych wjazdu/wyjazdu obywateli państw trzecich odwiedzających strefę Schengen (CESE 2016-03098, SOC/544, sprawozdawca: Pîrvulescu ([4])).

— **ETIAS: europejski system informacji o podróży oraz zezwoleń na podróż**, aktualnie oczekujący na decyzję, który ma być dużym automatycznym systemem do przechowywania i uprzedniej weryfikacji danych obywateli państw trzecich zwolnionych z obowiązku wizowego do celów poruszania się po strefie Schengen (CESE 2016-06889, SOC/556, sprawozdawca: Simons ([5])).

— **ECRIS-TCN: europejski system przekazywania informacji z rejestrów karnych dotyczących obywateli państw trzecich**, będący aktualnie przedmiotem wniosku Komisji – elektroniczny system wymiany informacji na temat orzeczeń sądowych wydanych już przez krajowe organy wymiaru sprawiedliwości.

2.5. Narzędzia dostępne obecnie dla uprawnionego organu można porównać do korzystania ze smartfona z różnymi aplikacjami, z których każda działa oddzielnie i dostarcza własne, niepowiązane z innymi informacje.

2.6. Systemy te – poza SIS – są skoncentrowane na **obsłudze obywateli państw trzecich**. Istnieje sześć uzupełniających się i zdecentralizowanych systemów. Na sumę poszukiwanych informacji składają się poszczególne odpowiedzi uzyskane z różnych baz przez służby śledcze w zależności od przyznanych im uprawnień dotyczących dostępu.

2.7. Komisja zamierza odpowiedzieć na następujące pytanie:

— jaką metodą, bez zmiany obecnych struktur i z zachowaniem ich komplementarności, kierować zapytania do wszystkich baz danych jednocześnie, aby w danym punkcie wjazdu na terytorium europejskie i za pomocą pojedynczego zapytania do systemu zebrać wszystkie dostępne już w istniejących bazach informacje i przekazać je organowi nadzoru posiadającemu uprawnienia do pytania o nie, zapewniając przy tym poszanowanie przepisów o ochronie danych i praw podstawowych

2.8. Cele Komisji Europejskiej w ramach analizowanych wniosków:

2.8.1. dodać możliwości, które stworzyłby dostęp do baz danych Europolu i Interpolu, które już współpracują z europejskimi organami nadzoru;

2.8.2. „zsynchronizować" wyszukiwanie informacji w celu skrócenia czasu reakcji w odniesieniu do spraw migrantów i, w razie konieczności, przyspieszenia reakcji służb bezpieczeństwa. Komitet proponuje, by w tym celu utworzyć nowe jednostki, które umożliwiłyby działanie w symbiozie istniejących baz.

2.9. **Celem Komisji jest zaradzenie w jak największym stopniu lukom w poszczególnych systemach**; poprawa zarządzania zewnętrznymi granicami strefy Schengen; wzmocnienie bezpieczeństwa wewnętrznego Unii; zajęcie się kradzieżami tożsamości, rozwiązanie kwestii multiplikacji tożsamości; odnalezienie osób podejrzanych lub już skazanych i kontrolowanie tożsamości tych osób w strefie Schengen.

2.10. Wracając do porównania do smartfona, uprawniony organ nie tylko będzie dysponował wieloma aplikacjami, ale będzie również mógł jednocześnie i w ramach tego samego wyszukiwania (za pomocą swych kodów dostępu) zebrać dane zgromadzone na wszystkich swoich nośnikach (komputerze stacjonarnym, laptopie, telefonie, tablecie, notebooku itp.).

([2]) Dz.U. C 34 z 2.2.2017, s. 144.
([3]) Dz.U. C 458 z 19.12.2014, s. 36.
([4]) Dz.U. C 487 z 28.12.2016, s. 66.
([5]) Dz.U. C 246 z 28.7.2017, s. 28.

3. **Działanie systemu**

3.1. Komisja rozpoczęła konsultacje i powołała grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności ([6]), wyznaczonych przez państwa członkowskie, państwa grupy Schengen, agencje europejskie, takie jak eu-LISA ([7]) i FRA ([8]), przy czym działania grupy koordynuje DG ds. Migracji i Spraw Wewnętrznych.

Właściwa metoda: połączenia wzajemne czy interoperacyjność?

3.1.1. **Połączenie wzajemne** systemów informacyjnych oznacza możliwość połączenia ich między sobą tak, by dane z jednego systemu mogły być automatycznie sprawdzane za pośrednictwem innego systemu.

3.1.2. **Interoperacyjność** ([9]) oznacza zdolność różnych systemów do komunikowania się, wymiany danych i wykorzystywania wymienionych danych, z poszanowaniem uprawnień dostępu do systemów.

3.2. *Wybór interoperacyjności*

3.2.1. Komisja uważa, że interoperacyjność nie zaburza dotychczasowego funkcjonowania struktur ani aktualnych kompetencji, a dane pozostaną w zabezpieczonych bazach. Pomimo zwiększonej zdolności komunikacji stanowiłoby to atut pod względem bezpieczeństwa dla systemów i danych, z których żaden nie będzie oczywiście dostępny przez internet. Omawiane teksty łączy wiele podobieństw.

— COM(2017) 793 odnosi się do interoperacyjności systemów informacyjnych dotyczących granic i wiz,

— natomiast COM(2017) 794 dotyczy współpracy między policją a wymiarem sprawiedliwości oraz azylu i migracji.

3.3. *Nowe narzędzia*

3.3.1. Aby zapewnić interoperacyjność, sześć stosowanych baz należy uzupełnić nową architekturą czterech nowych narzędzi. Chodzi o umożliwienie szybkiej pracy dzięki jednorazowemu zapytaniu do systemu, przy czym należy zagwarantować, że zapytania będą nadal przesyłane przez uprawnione osoby.

3.4. *ESP – europejski portal wyszukiwania*

3.4.1. Uprawniony organ nadzoru (użytkownik końcowy) powinien uzyskiwać jednocześnie dostęp do całości systemu. Zamiast przeprowadzać sześć wyszukiwań będzie przesyłać tylko jedno (policja, służby celne itp.), aby pozyskać informacje z szeregu baz na temat poszukiwanych danych, przy czym system nie będzie przechowywał tych danych. Jeśli dane istnieją, system je znajdzie. W wypadku podejrzenia o przestępstwo lub działalność terrorystyczną pierwsze trafienie może być neutralne dla kontrolowanej osoby („non-hit"), lecz jeśli informacja znajdzie potwierdzenie w drugiej informacji („hit") istniejącej w bazach takich jak SIS, EES, ETIAS, może to skutkować dalszym badaniem i śledztwem.

3.5. *Shared BMS – wspólny serwis kojarzenia danych biometrycznych*

3.5.1. Ta wspólna platforma służąca do celów dopasowywania danych będzie umożliwiała jednoczesne wyszukiwanie i porównywanie danych zmatematyzowanych, biometrycznych, linii papilarnych i zdjęć z dokumentów tożsamości z różnych baz zawierających takie dane, takich jak SIS, Eurodac, VIS, *EES* ([10]), *ECRIS*, ale nie *ETIAS*; zawarte w nich dane będą musiały być ze sobą kompatybilne.

3.5.2. Dane zmatematyzowane nie będą przechowywane w pierwotnej formie.

3.6. *CIR – wspólne repozytorium danych umożliwiających identyfikację*

3.6.1. We „wspólnym repozytorium danych umożliwiających identyfikację" będą gromadzone dane dotyczące tożsamości biograficznej i biometrycznej kontrolowanych osób będących obywatelami państw trzecich, znajdujących się na granicy lub w państwach członkowskich (strefy Schengen). Wskaźnik zgodności wyników w różnych bazach przyspieszy wyszukiwanie. Dane te będą zabezpieczone na odpowiedzialność i za pomocą środków bezpieczeństwa agencji eu-LISA, przy czym nikt nie będzie mógł uzyskać dostępu do więcej niż jednej linii alfanumerycznej jednocześnie. Repozytorium CIR powstanie na podstawie EES i ETIAS i nie powinno spowodować powielania danych. Repozytorium będzie także mogło służyć do wyszukiwań cywilnych.

([6]) DG ds. Migracji i Spraw Wewnętrznych, Dział B/3; decyzja Komisji C/2016/3780 z dnia 17 czerwca 2016 r.; http://ec.europa.eu/transparency/regexpert/index.cfm?Lang=PL.

([7]) Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości.

([8]) FRA: Agencja Praw Podstawowych Unii Europejskiej.

([9]) Komisja, COM(2016) 205 final, komunikat „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa".

([10]) Kursywę zastosowano w celu przypomnienia, że akty prawne dotyczące tych organów nie zostały jeszcze przyjęte.

3.7. *MID – moduł wykrywający multiplikację tożsamości*

3.7.1. Jego zadaniem będzie sprawdzanie prawdziwej tożsamości osób działających w dobrej wierze i zwalczanie oszustw dotyczących tożsamości przez przeszukiwanie wszystkich baz jednocześnie. Żaden organ nie korzystał jeszcze z podobnego narzędzia, które powinno umożliwić zapobieganie przywłaszczaniu tożsamości.

3.8. *Rola agencji eu-LISA* ([11])

3.8.1. Agencja powstała w 2011 r. i jej zadaniem jest ułatwianie realizacji polityki UE w dziedzinie wymiaru sprawiedliwości, bezpieczeństwa i wolności. Jej siedziba mieści się w Tallinie (Estonia). Zapewnia ona już wymianę informacji między różnymi organami ścigania w państwach członkowskich i ciągłe działanie wielkoskalowych systemów informatycznych, a także swobodę przemieszczania się osób w strefie Schengen.

3.8.2. Agencja pracuje nad projektem inteligentnych granic „Smart Borders", przy czym w nowej architekturze wymiany danych rola agencji będzie polegała na przechowywaniu elementów związanych z osobami, a także elementów dotyczących organów władzy, śledztw i śledczych. Będzie ona sprawdzała uprawnienia składających zapytania i zapewni bezpieczeństwo danych, także w przypadku „incydentu" (art. 44 we wnioskach COM(2017) 793 i 794).

3.8.3. **Zastosowanie uniwersalnego formatu wiadomości** UMF (Universal Message Format), który nie został jeszcze stworzony, ma ułatwić pracę z nowymi, obowiązkowymi systemami. Będzie się to wiązało z koniecznością utworzenia interfejsów w tych państwach członkowskich, które ich jeszcze nie mają, oraz tymczasowego systemu tłumaczenia z jednego języka na drugi.

3.9. *Ochrona danych osobowych* (art. 7 i 8 Karty)

3.9.1. W projekcie rozporządzenia uznaje się możliwość wystąpienia wypadków w dziedzinie bezpieczeństwa. Państwa członkowskie i krajowe systemy danych muszą w pierwszej kolejności stosować zasady ochrony danych przewidziane prawem, Traktatem, Kartą praw podstawowych oraz ogólnym rozporządzeniem o ochronie danych ([12]), które wejdzie w życie w dniu 25 maja 2018 r.

4. **Dyskusja**

4.1. *Wartość dodana interoperacyjności w demokracji*

4.1.1. UE potrzebuje regulacji i środków dochodzeniowych, które chronią przed przestępczością. Interoperacyjność systemów informacyjnych to szansa, by podkreślić nadrzędne znaczenie praworządności i ochrony praw człowieka.

4.1.2. *EES i ETIAS* powiązane z BMS i CIR pozwolą kontrolować przekraczanie granic przez osoby podejrzane, a także pozwolą przechowywać dotyczące ich dane. Jednakże możliwy „dostęp organów ścigania do systemów informacyjnych niezwiązanych ze ściganiem przestępstw na szczeblu UE" (art. 17 dotyczący CIR we wnioskach COM(2017) 794 i 793) nie jest zgodny z celami wskazanymi jako podstawy przedstawionych wniosków. Komitet (art. 300 ust. 4 TFUE) musi przywołać w tym miejscu zasadę proporcjonalności i wzywa Komisję, by nie tworzyła jakichkolwiek rozwiązań na wzór „Wielkiego Brata" ([13]) ani jakichkolwiek przeszkód dla swobody przemieszczania się Europejczyków (art. 3 TFUE).

4.1.3. Proponowany model gromadzenia i wykorzystywania danych osobowych pozyskanych na granicy i na terytorium Unii podczas kontroli przemieszczenia się i posiadanych dokumentów przedstawiono jako szczelny oraz dostępny wyłącznie dla uprawnionych osób i na potrzeby bezpieczeństwa i zarządzania; przyczyni się on ponadto do większej płynności procedur.

4.1.4. Niemniej kwestia szczelności budzi wątpliwości Komitetu: istniejące luki nie znikną, a budowa rozciągnięta na dziewięć lat opiera się na podstawach, które jeszcze nie istnieją, takich jak bazy EES, ETIAS czy interfejsy krajowe. Kontekst technologiczny ciągle się zmienia, a projekt opiera się z konieczności na obecnym stanie techniki i nie przewiduje środków budżetowych na radzenie sobie ze starzeniem się technologii w niektórych obszarach informatycznych.

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.U. L 286 z 1.11.2011, s. 1).

([12]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Opinie EKES-u: Dz.U. C 229 z 31.7.2012, s. 90 i Dz.U. C 345 z 13.10.2017, s. 138.

([13]) Pojęcie zaczerpnięte z książki „Rok 1984" George'a Orwella.

4.1.5. Ponadto można było uwzględnić w projekcie szybki postęp w stosowaniu algorytmów tzw. sztucznej inteligencji – do zastosowania zarówno jako narzędzie kontroli systemów, jak i jako klucz bezpieczeństwa dla organów decyzyjnych w celu zapewnienia demokratycznego wykorzystania architektury.

4.1.6. We wniosku ustanowiono system dla osób działających w dobrej wierze, szanujących prawo. To, że będą nim sterować ludzie, jest uspokajające, niemniej mogą oni okazać się jednocześnie słabym ogniwem systemu. Komitet sugeruje dodanie artykułu przewidującego swego rodzaju bezpieczniki na wypadek wystąpienia kryzysu politycznego lub kryzysu zarządzania, ponieważ każdy problem w pojedynczej bazie może stanowić ryzyko dla całej architektury systemu ([14]). Upowszechnienie UMF może doprowadzić do korzystania z systemu w skali międzynarodowej, bardzo pozytywnego, ale bardzo ryzykownego dla ochrony danych. Upoważnione organy ponosić będą wielką odpowiedzialność. Aspekty te nie zostały uwzględnione w omawianych wnioskach.

4.2. *Ochrona praw podstawowych*

4.2.1. Prawa podstawowe to prawa absolutne, ich ograniczenia „mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznanym przez Unię", z poszanowaniem istoty tych praw (art. 8 i art. 52 ust. 1 Karty). Komitet zastanawia się, w jaki sposób można ocenić proporcjonalność środków kontroli w przypadku migrantów uciekających przed prześladowaniami i pragnących uzyskać azyl w Unii. (COM(2017) 794 final – Uzasadnienie – Prawa podstawowe). Poszukiwanie osób podejrzanych w celu zapobiegania przestępstwom, w szczególności terrorystów, **nie może przybliżać naszych demokracji do koncepcji wyprzedzającego domniemania winy**. Należy zachować rozróżnienie między działaniami zakłócającymi porządek publiczny a opiniami.

4.2.2. Poszanowanie praw wymienionych w Karcie w odniesieniu do każdej osoby musi gwarantować równowagę między bezpieczeństwem a wolnością, bez której to równowagi demokracja umiera. Komitet uważa, że ta równowaga ma zasadnicze znaczenie i powinna być stale aktualnym celem dla wszystkich władz, w tym i dla organów nadzorczych – zarówno na poziomie krajowym, jak i europejskim.

4.2.3. Informacje na temat szeregu organów zaangażowanych w dane wyszukiwanie oraz powiązane metadane będą przechowywane w systemie. Należy zapewnić również poszanowanie praw podstawowych przysługujących uprawnionym organom w odniesieniu do generowanych danych, w szczególności w zakresie bezpieczeństwa i życia prywatnego, w przypadku włamania do struktury systemu i niewłaściwego wykorzystania danych – od momentu pozyskania tych danych do momentu usunięcia.

4.3. *Ochrona danych*

4.3.1. We wnioskach potwierdzono zasadę ochrony danych osobowych już w fazie projektowania i domyślnie, choć w uzasadnieniu przypomniano, że – jak stwierdził Trybunał – ochrona danych osobowych nie jest prawem absolutnym. Komitet docenia korzyści płynące ze środków zapobiegawczych gwarantujących bezpieczeństwo, ze zwalczania oszustw dotyczących tożsamości i z gwarantowania prawa azylu. Niemniej podkreśla ograniczenia matematyzacji i anonimizacji danych: osoby, których dane dotyczą, mogą ich w przyszłości potrzebować.

4.3.2. Podkreśla także, że rodzaj przechowywanych danych, biometrycznych i biologicznych, ma szczególną wartość dla niektórych przedsiębiorstw i dla świata przestępczego. W tym przypadku cyberbezpieczeństwo jest tak samo istotne jak bezpieczeństwo fizyczne, a we wnioskach mówi się o nim zbyt mało. Przechowywane dane będą gromadzone w jednej fizycznej lokalizacji, która mimo najlepszych zabezpieczeń zawsze jest narażona na pewne zagrożenia.

4.3.3. Odnośnie do ochrony danych i prawa do usunięcia danych (do bycia zapomnianym) EKES przypomina, że instytucje i organy Unii są zobowiązane do przestrzegania rozporządzenia (WE) nr 45/2001 zapewniającego niższy poziom ochrony niż ogólne rozporządzenie o ochronie danych z 2016 r. ([15]), które wchodzi w życie w maju 2018 r. i którego muszą przestrzegać państwa członkowskie. Komitet podkreśla złożony charakter wdrażania tych przepisów i obawia się, że podróżujący, migranci i osoby ubiegające się o azyl nie będą w stanie egzekwować ich przestrzegania:

1) ochrona danych osobowych musi zostać zatwierdzona dla wszystkich istniejących baz – krajowych i europejskich – aby ochronie podlegała całość;

2) ochrona jest kwestią podstawową, aby obywatele zgodzili się na wprowadzenie tej wszechobecnej machiny nadzoru.

4.3.4. We wnioskach nie określono wyraźnie okresu przechowywania danych zgromadzonych przez uprawnione organy. W tekstach jest mowa o procedurze realizującej prawo do sprostowania danych lub usunięcia danych, która angażuje państwo, do którego skierowano wniosek, i państwo odpowiedzialne, ale nie określa okresu przechowywania danych (art. 47 wniosków). Komitet zaleca, aby określono ten okres i aby był on krótszy w przypadku osób małoletnich (art. 24 Karty) – z wyłączeniem przypadków terroryzmu – tak aby osoby te mogły mieć szanse na integrację.

([14]) EIOD, załącznik, sprawozdanie końcowe grupy ekspertów wysokiego szczebla, maj 2017 r.
([15]) Ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679).

4.4. *Zarządzanie i obowiązek sprawozdawczości*

4.4.1. Bazy międzynarodowe nie podlegają tym samym regułom co europejskie systemy informatyczne. Wprowadzenie uniwersalnego formatu dostępu, który mógłby stać się międzynarodowy, będzie jedynie elementem technicznym, który nie ujednolici przepisów – nawet jeżeli Interpol na pewno przestrzega art. 17 paktu ONZ ([16]). Ponadto uprawnienia nadal pozostaną w gestii państw członkowskich. EKES uważa, że kwestię tę należało poruszyć we wnioskach.

4.4.2. Jedno zapytanie i połączone bazy europejskie wydadzą werdykt. EKES zwraca uwagę, że związana z tym biurokracja będzie bardziej niż proporcjonalna w stosunku do wzrostu prędkości. Zarządzaniem zajmie się Komisja w ramach procedury kontroli wraz z państwami członkowskimi. Centralnym elementem systemu będzie agencja eu-LISA, odpowiedzialna przede wszystkim za wdrożenie procedur gromadzenia informacji na temat funkcjonowania interoperacyjności. Będzie ona otrzymywać informacje z państw członkowskich i Europolu oraz przedkładać Radzie, Parlamentowi Europejskiemu i Komisji co cztery lata sprawozdanie z oceny technicznej, przy czym Komisja przygotuje sama rok później sprawozdanie ogólne (art. 68 wniosków). Według Komitetu okresy te są zdecydowanie zbyt długie. Ocena bezpieczeństwa elementów interoperacyjności (art. 68 ust. 5 lit. d)) powinna odbywać się przynajmniej co roku, a ocena wpływu na prawa podstawowe przynajmniej co dwa lata (art. 68 ust. 5 lit. b)).

4.4.3. Komitet ubolewa, że tak zasadnicze kwestie jak te poruszane we wnioskach leżą w gestii agencji europejskich, w których zasady zatrudniania i funkcjonowania są niejasne dla wielu obywateli. Uważa, że konieczna jest wymiana dobrych praktyk i zwrócenie się o opinię do wszystkich niezależnych organów nadzorujących korzystanie z danych (EIOD) oraz do innych agencji, takich jak FRA i ENISA.

4.4.4. Wszystkie te nowe struktury i procedury zostaną wprowadzone na podstawie aktów delegowanych i aktów wykonawczych Komisji. Komitet chciałby, aby dążenie do poszanowania praw podstawowych i ochronę danych osobowych zapisano we wszystkich tych kolejnych aktach z myślą o coraz lepszym podejściu do przyjmowania osób na granicach. EKES zaleca, aby obywatele europejscy byli informowani o realizacji kolejnych etapów projektu aż do jego zakończenia, i by osobom podlegającym kontrolom udzielano informacji wyjaśniających na temat tych kontroli.

5. **Niezbędne szkolenia dla organów nadzorczych w całej Unii**

5.1. Komitet uważa, że na początkowym etapie (po 2021 r.) konieczne będą liczne szkolenia, wbrew zapowiedzi Komisji w jej podsumowaniu oceny skutków (*C*). Komisja wspomina o 76 mln EUR rocznie. Przejście do stosowania nowych procedur zawsze wymaga aktualizacji. W tym wypadku chodzi o wszystkie granice Unii i systemy krajowe. Niektóre państwa członkowskie nie posiadają jeszcze kompatybilnych systemów, więc będą musiały zdobyć się na duży wysiłek i stworzyć interfejsy umożliwiające im uczestnictwo w systemie. Aby interoperacyjność stała się faktem, usunięte muszą zostać różnice między państwami członkowskimi.

5.2. Szkolenie z korzystania z danych wysokiej jakości i z zakresu UMF będzie miało zasadnicze znaczenie. Komitet sugeruje zorganizowanie razem z CEPOL-em ([17]), Fronteksem oraz Europolem ośrodka wspólnych szkoleń dla uprawnionych organów, w tym dla agencji eu-LISA, której członkowie powinni mieć wnikliwie sprawdzane kwalifikacje.

5.3. Narzędzie takie jak MID nie istnieje nigdzie indziej. W przypadku sukcesu będzie to narzędzie o wielkiej mocy. Nowa architektura będzie wymagać jak największej jakości danych. Aby spełniły się nadzieje pokładane w projekcie, wszystkie państwa członkowskie muszą uczestniczyć na tym samym poziomie, w przeciwnym wypadku luki będą jeszcze poważniejsze niż dotychczas. Wówczas zagrożone byłoby prawo do azylu i prawo do ochrony międzynarodowej (art. 18 i 19 Karty).

6. **Finansowanie**

6.1. Cała proponowana architektura opiera się na kilku założeniach: przyjęcie przez organy decyzyjne systemów *EES*, *ETIAS*, *UMF*, prawidłowe funkcjonowanie *MID* i zabezpieczenie *CIR*. Czy dwa organy, EIOD i agencja eu-LISA, a być może także agencja ENISA, będą dysponować wystarczającymi zasobami ludzkimi i finansowymi? Komisja proponuje współfinansowanie ze strony UE i państw członkowskich. Komitet zwraca uwagę, że zarządzanie europejskim semestrem odbywa się nadal pod znakiem polityki oszczędnościowej oraz że obecne wykorzystanie istniejących baz (SIS, VIS, Prüm, *EES*) należy jeszcze zoptymalizować zgodnie z wymogami prawnymi (sprawozdanie grupy ekspertów).

([16]) Międzynarodowy pakt praw obywatelskich i politycznych ONZ, „Artykuł 17. 1. Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. 2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami".

([17]) CEPOL, Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania (Budapeszt, Węgry).

6.2. EKES zastanawia się nad skutkami budżetowymi brexitu, mimo że Zjednoczone Królestwo nie należy do systemu Schengen, a w bardziej ogólnym ujęciu, nad przyszłym stopniem złożoności zarządzania interoperacyjnością w krajach europejskich nienależących do SIS, lecz uczestniczących w innych systemach takich jak Eurodac.

6.3. Przewidzianym funduszem jest Fundusz Bezpieczeństwa Wewnętrznego – granice i wizy. Uruchomienie Funduszu przewidziano na 2023 r. Komitet zastanawia się, czy okres pięciu lat wystarczy na zmniejszenie zróżnicowania w Europie i stworzenie warunków gwarantujących powodzenie projektu. Planowany budżet wynosi 424,7 mln EUR na dziewięć lat (2019–2027). Kwotę ma uiścić Unia (Fundusz Bezpieczeństwa Wewnętrznego – granice i wizy) i państwa członkowskie. Państwa członkowskie muszą zapewnić prawidłowe funkcjonowanie istniejących systemów z nową architekturą informatyczną. Komitet uważa, że ożywienie gospodarcze powinno przyczynić się do realizacji tych inwestycji.

Bruksela, dnia 23 maja 2018 r.

Luca JAHIER
Przewodniczący
Europejskiego Komitetu Ekonomiczno-Społecznego