Kwartalnik Kolegium Ekonomiczno-Społecznego „Studia i Prace”

№1(37)2019
s. 143–165
DOI: 10.33119/KKESSiP/2019.1.7

Anastazja Gajda
Wydział Prawa i Administracji
Uniwersytet Opolski
e-mail autora: agajda@uni.opole.pl

INTEROPERACYJNOŚĆ UNIJNYCH SYSTEMÓW INFORMACYJNYCH W ZAKRESIE BEZPIECZEŃSTWA, OCHRONY GRANIC I ZARZĄDZANIA MIGRACJAMI[1]

Streszczenie

W ciągu ostatnich lat w Unii Europejskiej (UE) coraz częściej dochodzi do przypadków nielegalnego przekraczania granic. Kontrole osób na granicach zewnętrznych UE powinny być zatem bardziej skuteczne, aby umożliwić m.in. efektywne zarządzanie migracjami. Szczególnie pilna stała się potrzeba połączenia i kompleksowego wzmocnienia unijnych narzędzi informacyjnych służących zarządzaniu granicami zewnętrznymi oraz zapobiegania nielegalnej migracji i jej zwalczania. Artykuł dotyczy kwestii zapewniania interoperacyjności wszystkich scentralizowanych systemów informacyjnych działających w przestrzeni wolności, bezpieczeństwa i sprawiedliwości UE. Okazuje się bowiem, że istniejące systemy nie współpracują ze sobą. Dlatego jako komponenty interoperacyjności zaproponowano: europejski portal wyszukiwania, wspólny serwis kojarzenia danych biometrycznych, wspólne repozytorium tożsamości i moduł wykrywający multiplikację tożsamości.

Słowa kluczowe: Unia Europejska, systemy informacyjne, ochrona granic zewnętrznych, interoperacyjność, przestrzeń wolności, bezpieczeństwa i sprawiedliwości

Artykuł nadesłany w listopadzie 2018 r., zaakceptowany w lutym 2019 r.

[1] Artykuł oddaje stan prawny na dzień 1 września 2018 r.

Wprowadzenie

Decyzja o zniesieniu kontroli na granicach wewnętrznych państw członkowskich Unii Europejskiej (dalej: UE lub Unia) pociągała za sobą konieczność wzmocnienia ochrony jej granic zewnętrznych, m.in. poprzez ustanowienie wielkoskalowych systemów informacyjnych w celu lepszego monitorowania przepływu osób do i z Unii oraz usprawnienia współpracy policyjnej i sądowej w sprawach transgranicznych[2]. W ciągu ostatnich dziesięcioleci w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej (dalej: PWBiS) utworzono wiele scentralizowanych systemów informacyjnych służących przechowywaniu danych osobowych obywateli państw trzecich, którzy chcą dostać się do strefy Schengen. Tendencja do rozszerzania już istniejących baz danych, a także do tworzenia nowych systemów informacyjnych o podobnych celach przypuszczalnie będzie się nasilała. Można już dziś zauważyć zwiększenie częstotliwości propozycji tworzenia kolejnych baz danych na szczeblu UE.

Bazy danych istniejące w ramach PWBiS obejmują systemy informatyczne, w których przechowuje się: dane osobowe do celów azylowych, informacje o osobach podróżujących i wizach oraz dane dotyczące osób zaginionych i przestępców. Wszystkie te systemy umożliwiają dostęp do przechowywanych w nich danych także organom ścigania państw członkowskich UE, tak aby mogły je wykorzystywać w trakcie działań związanych z zapobieganiem poważnym przestępstwom, ich wykrywania i prowadzenia w ich sprawie dochodzeń, leżących w granicach ich kompetencji.

Systemy informacyjne UE tworzono na przestrzeni wielu lat przede wszystkim z myślą o zapewnianiu bezpieczeństwa, a także kontroli granic oraz migracji. Każdy z systemów cechują odrębne: cele, zadania, podstawy prawne, zasady tworzenia i korzystania z nich, grupy użytkowników i kontekst instytucjonalny. Obecnie istnieją cztery scentralizowane systemy, tj. System Informacyjny Schengen (dalej: SIS)[3], system Eurodac[4], Wizowy System Informacyjny (dalej: VIS)[5] i System Wjazdu/Wyjazdu

[2] T. Quintel, *Connecting personal data of Third Country Nationals. Interoperability of EU databases in the light of the CJEU's case law on data retention*, „Law Working Paper Series" 2018, no. 2, s. 2, https://www.researchgate.net/publication/323924372_Connecting_Personal_Data_of_Third_Country_Nationals_Interoperability_of_EU_Databases_in_the_Light_of_the_CJEU's_Case_Law_on_Data_Retention [dostęp 01.09.2018].

[3] Obejmuje szerokie spektrum wpisów dotyczących osób (są to informacje dotyczące: odmowy wjazdu lub pobytu, europejskiego nakazu aresztowania, osób zaginionych, pomocy w prowadzeniu postępowań sądowych, kontroli niejawnych i kontroli szczególnych) oraz przedmiotów (w tym zagubionych, skradzionych lub unieważnionych dokumentów tożsamości lub podróży).

[4] Zawiera dane daktyloskopijne osób ubiegających się o azyl oraz obywateli państw trzecich, którzy nielegalnie przekroczyli granicę zewnętrzną lub nielegalnie przebywają w państwie członkowskim UE.

[5] Zawiera dane dotyczące wiz krótkoterminowych.

(dalej: EES)[6]. Planowane jest utworzenie dwóch kolejnych systemów, tj. europejskiego systemu informacji o podróży oraz zezwoleń na podróż (dalej: ETIAS)[7] oraz europejskiego systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (dalej: ECRIS-TCN)[8]. O kształcie tych systemów zadecydowały szczególne potrzeby w momencie ich tworzenia oraz instytucjonalne, polityczne i prawne konteksty, w których potrzeby te zostały zgłoszone[9]. Wskazane systemy pomagają władzom krajowym w zarządzaniu granicami i migracją, w rozpatrywaniu wniosków wizowych i azylowych oraz w zwalczaniu przestępczości i terroryzmu.

Systemy informacyjne UE nie są ze sobą połączone. Narzędzia, z których korzystają obecnie uprawnione organy, można porównać do smartfonu z różnymi aplikacjami, z których każda działa odrębnie i dostarcza własnych, niepowiązanych z innymi informacji. W zasadzie wszystkie te systemy (poza systemem SIS) są skoncentrowane na obsłudze obywateli państw trzecich. Na sumę poszukiwanych informacji składają się poszczególne odpowiedzi uzyskane z różnych baz przez służby śledcze w zależności od przyznanych im uprawnień dotyczących dostępu.

Systemy mają jednak podobne cechy. Z wyjątkiem proponowanego systemu ETIAS wszystkie istniejące bazy danych przechowują dane biometryczne (odciski palców oraz obrazy twarzy). Ze względu na swój szczególnie wrażliwy charakter dane biometryczne mogą być przetwarzane tylko w ściśle określonych warunkach i są objęte silniejszymi gwarancjami ochrony danych[10]. Informacje przechowuje się przez podobny okres, tj. od 3 do 5 lat albo dłużej. Jeżeli dane są dostępne przez porównywalne okresy, to właściwe organy uzyskujące dostęp do tych danych i przetwarzające je mogą tworzyć bardzo szczegółowe profile.

W niniejszym artykule zostanie przeanalizowany problem zapewniania interoperacyjności między wszystkimi wskazanymi systemami informacyjnymi funkcjonującymi

---

[6] Zastąpi obecny system ręcznego umieszczania odcisków pieczęci w paszportach i będzie elektronicznie rejestrować: nazwisko, rodzaj dokumentu podróży, dane biometryczne, a także datę i miejsce wjazdu oraz wyjazdu obywateli państw trzecich odwiedzających strefę Schengen w celu krótkiego pobytu. Ma być w pełni operacyjny do końca 2020 r.

[7] Będzie to w znacznej mierze automatyczny system służący gromadzeniu i weryfikacji informacji dostarczanych przez obywateli państw trzecich zwolnionych z obowiązku wizowego (ma to następować przed odbyciem przez nich podróży do strefy Schengen). W trakcie prac redakcyjnych dotyczących niniejszego artykułu zostało przyjęte rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226, Dz. Urz. UE 2018 L 236/1.

[8] Będzie to elektroniczny system wymiany informacji dotyczących wcześniejszych wyroków skazujących wydanych przeciwko obywatelom państw trzecich przez sądy karne w UE.

[9] Zob. European Data Protection Supervisor statement on the concept of interoperability in the field of migration, asylum and security, https://edps.europa.eu/sites/edp/files/publication/17-05-08_statement_on_interoperability_en.pdf [dostęp 01.09.2018].

[10] T. Quintel, op.cit., s. 9.

w ramach PWBiS. Jak już bowiem wspomniano, systemy informacyjne nie są obecnie interoperacyjne, tj. zdolne do wymiany danych i dzielenia się informacjami tak, aby władze i właściwi urzędnicy dysponowali potrzebnymi im informacjami w czasie i w miejscu, w których ich potrzebują. W niniejszym opracowaniu omówiono genezę i kontekst kompleksowego wzmocnienia unijnych narzędzi informacyjnych służących zarządzaniu granicami i migracją oraz zapewnianiu bezpieczeństwa wewnętrznego UE. Przedstawiono także projekty rozporządzeń ustanawiających ramy interoperacyjności między unijnymi systemami informacyjnymi, przewidujące stworzenie: europejskiego portalu wyszukiwania, wspólnego serwisu kojarzenia danych biometrycznych, wspólnego repozytorium danych identyfikacyjnych oraz modułu wykrywającego multiplikację tożsamości.

1. Interoperacyjność systemów informacyjnych funkcjonujących w ramach PWBiS – geneza i kontekst

Dyskusje na temat interoperacyjności systemów informacyjnych funkcjonujących w PWBiS zaczęły się po atakach terrorystycznych z 11 września 2001 r.[11] i głównie skupiały się na tym, czy VIS (który był wtedy w fazie negocjacji) mógłby być interoperacyjny z systemem SIS[12]. Po zamachach bombowych w Madrycie w 2004 r. Rada Europejska wezwała Komisję Europejską „do przedstawienia propozycji dla wzmocnienia interoperacyjności europejskich baz danych i zbadania możliwości ustanowienia synergii pomiędzy istniejącymi i przyszłymi systemami"[13]. Podobne wezwanie pojawiło się także w Programie haskim[14], jak i w deklaracji Rady UE z 13 lipca 2005 r.[15], wydanej po atakach terrorystycznych w Londynie.

W listopadzie 2005 r. Komisja opublikowała komunikat w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych[16].

---

[11] Zob. Council of the European Union, Additional measures to combat terrorism – proposals by the German delegation, 13176/01, Brussels, 24.10.2001.

[12] European Commission, Development of the Schengen Information System II, COM(2001) 720 final, Brussels, 18.12.2001, s. 8.

[13] Council of the European Union, Declaration on combating terrorism, 7906/04, Brussels, 29.03.2004.

[14] Zob. Rada, Program haski: wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, Dz. Urz. UE 2005 C 53/01. Program ten przewidywał plan działań w dziedzinie PWBiS na lata 2005–2009.

[15] Council of the European Union, Declaration condemning the terrorists attacks on London, 11116/05, Brussels, 13.07.2005 (Presse 187).

[16] Komisja Europejska, Komunikat w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw

Skupiając się na operacyjności systemów VIS, SIS i Eurodac, najpierw zwięźle opisywano aktualny stan systemów informacyjnych oraz zidentyfikowano ich braki. Następnie przedstawiono możliwości wykorzystywania tych systemów w sposób bardziej efektywny, a także możliwości utworzenia ewentualnych nowych systemów informacyjnych[17].

Podstawowym celem komunikatu było „zwrócenie uwagi na możliwości bardziej efektywnego wykorzystania tych systemów w realizacji polityki w zakresie swobodnego przepływu osób oraz celów związanych ze zwalczaniem terroryzmu i poważnej przestępczości w sposób wykraczający poza obecne przeznaczenie tych systemów"[18]. Paralelnie rozważano także konieczność znalezienia odpowiedniej równowagi pomiędzy dążeniem do realizacji tych celów a ochroną praw podstawowych jednostki (w szczególności ochroną danych osobowych) zgodnie z postanowieniami Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.) oraz Karty praw podstawowych Unii Europejskiej (Dz. Urz. UE 2012 C 326/391; dalej: KPP).

Komisja w komunikacie przedstawiła także swoją koncepcję interoperacyjności, traktując ją jako „możliwość wymiany danych, informacji i wiedzy pomiędzy systemami informacyjnymi oraz procesami operacyjnymi realizowanymi przy pomocy tych systemów"[19]. Jednocześnie, bez przeprowadzenia dyskusji na temat możliwości użycia tej definicji w PWBiS, Komisja uznała, że „interoperacyjność to pojęcie bardziej techniczne niż prawne czy polityczne. Nie uwzględnia ono kwestii, czy wymiana danych jest zgodna z prawem, możliwa ze względów politycznych lub wymagana"[20].

Komunikat spotkał się z ostrą krytyką m.in. ze strony Europejskiego Inspektora Ochrony Danych Osobowych (dalej: EIOD)[21]. Wątpliwości budziła już sama definicja interoperacyjności, którą EIOD uznał za niejednoznaczną i nie do końca jasną. Ponadto nie podzielał on w pełni poglądu, że interoperacyjność jest raczej kwestią techniczną, a nie prawną lub polityczną. Istotne zastrzeżenia dotyczyły także

wewnętrznych, COM(2005) 597 final, Bruksela, 24.11.2005.

[17] Zob. European Parliament, Interoperability of Justice and Home Affairs Information Systems. Study, April 2018, s. 45, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf [dostęp 01.09.2018].

[18] Komisja Europejska, Komunikat w sprawie zwiększenia skuteczności…, op.cit., s. 2.

[19] W tym celu Komisja skorzystała z definicji zawartej w Europejskich Ramach Interoperacyjności dla Transeuropejskich Usług Administracji Elektronicznej, Urząd Oficjalnych Publikacji Wspólnot Europejskich, 2004, punkt 1.1.2.

[20] Komisja Europejska, Komunikat w sprawie zwiększenia skuteczności…, op.cit., s. 4.

[21] European Data Protection Supervisor, Comments on the Communication of the Commission on interoperability of European databases, Brussels, 10.03.2006, https://edps.europa.eu/sites/edp/files/publication/06–03-10_interoperability_en.pdf [dostęp 01.09.2018].

potencjalnych konsekwencji wprowadzenia interoperacyjności dla praw podstawowych jednostki, zwłaszcza w zakresie ochrony danych osobowych[22].

W kolejnej dekadzie zostały podjęte bardzo ograniczone działania w celu osiągnięcia interoperacyjności systemów informacyjnych UE. Nastąpiły jednak znaczące zmiany w odniesieniu do środowiska tych systemów w PWBiS. Ustanowiono systemy VIS[23], SIS II[24] i ECRIS[25].

Dopiero po kolejnych zamachach terrorystycznych na terytorium Unii (w Paryżu w 2015 r. i w Brukseli w 2016 r.) dyskusje na temat interoperacyjności nabrały nowego impetu. W rezultacie w latach 2015–2017 odpowiednie instytucje unijne prezentowały swoje stanowiska w tej dziedzinie, m.in. w licznych konkluzjach Rady Europejskiej[26], Planie działania Rady[27] czy wspólnym oświadczeniu ministrów UE ds. sprawiedliwości i spraw wewnętrznych[28].

W 2016 r. Komisja opublikowała komunikat: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa[29], w którym wskazywała, jak dzięki systemom informacyjnym można poprawić zarządzanie granicami i migracją oraz zapewnić bezpieczeństwo wewnętrzne w UE. W komunikacie stwierdzono także kilka strukturalnych błędów dotyczących

---

[22] Zob. też P. De Hert, S. Gurtwirth, *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, „International Review of Law Computers and Technology" 2006, vol. 20, issue 1–2, s. 31–32.

[23] Zob. decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz. Urz. UE 2004 L 213/5.

[24] Zob.: rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE 2006 L 381/4; decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE 2007 L 205/63; rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE 2006 L 381/1.

[25] Zob.: decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, Dz. Urz. UE 2009 L 93/23; decyzja Rady 2009/316/WSiSW z dnia 6 kwietnia 2009 r. w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW, Dz. Urz. UE 2009 L 93/33.

[26] European Council, European Council meeting (17 and 18 December 2015) – Conclusions, EUCO 28/15, Brussels, 18.12.2015; European Council, European Council meeting (15 December 2016) – Conclusions, EUCO 34/16, Brussels, 15.12.2016.

[27] Council of the European Union, Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, 9368/1/16, Brussels, 06.06.2016.

[28] Rada Unii Europejskiej, Wspólne oświadczenie unijnych ministrów sprawiedliwości i spraw wewnętrznych oraz przedstawicieli instytucji UE w sprawie zamachów terrorystycznych, do których doszło w Brukseli 22 marca 2016 r., 7371/16, Bruksela, 24.03.2016.

[29] Komisja Europejska, Komunikat: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, COM(2016) 205, Bruksela, 06.04.2016.

tych systemów. Zdaniem KE niektóre z istniejących systemów informacyjnych mają nieoptymalne mechanizmy działania. Ponadto w unijnej architekturze zarządzania danymi istnieją luki informacyjne. Systemy informacyjne są zarządzane w różny sposób i tworzą skomplikowany układ. W końcu zarządzanie danymi dotyczącymi granic i bezpieczeństwa odbywa się w ramach fragmentarycznych struktur, a informacje przechowywane są oddzielnie w niepowiązanych systemach, co sprawia, że pewne dane pozostają nieuwzględnione.

W czerwcu 2016 r. Komisja powołała grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności[30]. Jej podstawowym zadaniem było przygotowanie raportu określającego zakres wyzwań prawnych, technicznych i operacyjnych związanych z poprawą interoperacyjności między centralnymi systemami informacyjnymi UE służącymi ochronie granic i zapewnianiu bezpieczeństwa.

Raport ten grupa ekspertów zaprezentowała w maju 2017 r.[31] Określono w nim serię zaleceń, mających na celu wzmocnienie i rozwój unijnych systemów informacyjnych i ich interoperacyjność[32]. Generalnie uznano, że prace nad praktycznymi rozwiązaniami służącymi zapewnieniu interoperacyjności systemów informacyjnych są konieczne i możliwe do wykonania pod względem technicznym. Przyjęcie odpowiednich rozwiązań w tym zakresie zgodnych z wymogami dotyczącymi ochrony danych osobowych może przynieść wymierne korzyści operacyjne.

W swoich konkluzjach z 22–23 czerwca 2017 r.[33] Rada Europejska zwróciła się do Komisji, by ta jak najszybciej przygotowała projekty aktów prawnych wprowadzających w życie propozycje grupy ekspertów. W kontekście swojego programu prac na 2018 r.[34] Komisja ogłosiła, że do końca 2017 r. przedstawi wniosek w sprawie interoperacyjności systemów operacyjnych, aby wzmocnić działania na rzecz uczynienia społeczeństwa UE bezpieczniejszym, przy pełnym poszanowaniu praw podstawowych.

---

30 Zob. decyzja Komisji z dnia 17 czerwca 2016 r. ustanawiająca grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności (2016/C 257/03), Dz. Urz. UE 2016 C 257/03.

31 Zob. *High-level expert group on information systems and interoperability. Final report*, 2017 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1 [dostęp 01.09.2018].

32 W pracach grupy ekspertów aktywnie uczestniczyli: Agencja Praw Podstawowych Unii Europejskiej, EIOD i Koordynator UE ds. Zwalczania Terroryzmu. Wszyscy wyrazili swoje poparcie, przyznając jednocześnie, że w dalszych pracach należy uwzględnić szersze kwestie związane z ochroną praw podstawowych jednostki i danych osobowych. Przedstawiciele Sekretariatu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego oraz Sekretariatu Generalnego Rady uczestniczyli w posiedzeniach grupy jako obserwatorzy.

33 European Council, European Council meeting (22 and 23 June 2017) – Conclusions, EUCO 8/17, Brussels, 23.06.2017.

34 Komisja Europejska, Program prac Komisji na 2018 r. Plan działania na rzecz bardziej zjednoczonej, silniejszej i bardziej demokratycznej Unii, COM(2017) 650 final, Bruksela, 24.10.2017.

2. Wnioski w sprawie interoperacyjności – najważniejsze założenia

Komisja przedstawiła 12 grudnia 2017 r. dwa wnioski legislacyjne w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE[35]. Pierwszy z nich dotyczy wielkoskalowych systemów informacyjnych odnoszących się do granic i wiz, tj. systemów EES, VIS, ETIAS i SIS (dalej: wniosek nr 1)[36]. Drugi wniosek obejmuje systemy informacyjne odnoszące się do współpracy policyjnej i sądowej, azylu i migracji, tj. systemów Eurodac, SIS oraz ECRIS-TCN (dalej: wniosek nr 2)[37]. Oprócz tych systemów informacyjnych, zarządzanych centralnie na szczeblu Unii,

[35] Publikacja dwóch wniosków legislacyjnych zamiast jednego wynikała z konieczności przestrzegania rozróżnienia między systemami, które dotyczą z jednej strony dorobku Schengen dotyczącego granic i wiz, tj. systemów VIS, EES, ETIAS i SIS, regulowane rozporządzeniem (WE) nr 1989/2006, i z drugiej strony dorobku Schengen w sprawie współpracy policyjnej, i tymi, które nie są związane z dorobkiem Schengen (systemy Eurodac, ECRIS-TCN oraz SIS, regulowane decyzją Rady 2007/533/WSiSW).

[36] Zob.: wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399 i rozporządzenie (UE) 2017/2226, Strasburg, 12.12.2017, COM(2017) 793. W czerwcu 2018 r. Komisja przedstawiła zmieniony wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399, rozporządzenie (UE) 2017/2226, rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie ETIAS], rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie SIS w odniesieniu do odpraw granicznych] oraz rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie eu-LISA], COM(2018) 478, Bruksela, 13.06.2018. W rozdziale IX tego zmienionego wniosku wprowadzono zmiany do pierwotnego wniosku jedynie w zakresie, w jakim stanowią one dalsze niezbędne zmiany innych aktów prawnych wymagane w związku z projektem rozporządzenia w sprawie interoperacyjności. Zmiany te uznano za niezbędne już w pierwotnym wniosku, ale ze względu na toczące się negocjacje między współustawodawcami w sprawie niektórych systemów niemożliwe było uwzględnienie tych niezbędnych zmian w pierwotnym wniosku. Z proponowanych zmian wynika z kolei konieczność aktualizacji oceny skutków finansowych regulacji. Dalsza analiza będzie prowadzona na podstawie pierwotnego wniosku.

[37] Wniosek rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja), Strasburg, 12.12.2017, COM(2017) 794 final. W czerwcu 2018 r. Komisja przedstawiła zmieniony wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja) oraz zmieniające [rozporządzenie (UE) 2018/XX [rozporządzenie Eurodac], rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie SIS w odniesieniu do ścigania przestępstw], rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie ECRIS-TCN] oraz rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie eu-LISA], COM(2018) 480, Bruksela, 13.06.2018. W rozdziale VIIIa niniejszego wniosku wprowadzono zmiany do pierwotnego wniosku jedynie w zakresie, w jakim stanowią one dalsze niezbędne zmiany innych aktów prawnych wymagane w związku z projektem rozporządzenia w sprawie interoperacyjności. Zmiany te uznano za niezbędne już w pierwotnym wniosku, ale ze względu na toczące się negocjacje między współustawodawcami w sprawie niektórych systemów niemożliwe było uwzględnienie tych niezbędnych zmian w pierwotnym wniosku. Z proponowanych zmian wynika z kolei konieczność aktualizacji oceny skutków finansowych regulacji. Dalsza analiza będzie prowadzona na podstawie pierwotnego wniosku.

zakres wniosków nr 1 i 2 (por. art. 3 obu dokumentów) obejmuje także bazę Interpolu (zawierającą dane skradzionych lub utraconych dokumentów podróży) oraz dane Europolu (jeżeli są one istotne z punktu widzenia funkcjonowania proponowanego systemu ETIAS oraz pomocy państwom członkowskim w przeglądaniu danych dotyczących poważnych przestępstw i terroryzmu).

W zasadzie wnioski nr 1 i 2 mogą być traktowane jako „bliźniacze propozycje", które można odczytywać razem. Numeracja artykułów jest zasadniczo podobna w obu wnioskach, podobnie jak ich treść. Oba dokumenty mają służyć poprawie zarządzania granicami zewnętrznymi strefy Schengen[38] oraz przyczynić się do zwiększenia bezpieczeństwa wewnętrznego UE[39]. W związku z tym tworzą one ramy interoperacyjności dla istniejących i przyszłych wielkoskalowych systemów informacyjnych UE. Na interoperacyjność między tymi systemami składałyby się cztery elementy, tj.:

1) **europejski portal wyszukiwania** (dalej: EPW) – działałby jako pośrednik komunikatów; jego podstawowym celem ma być zapewnienie prostego interfejsu, który szybko i w przejrzysty sposób dostarczałby wyniki zapytań; pozwoliłoby to na jednoczesne wyszukiwanie danych w różnych systemach przy użyciu danych identyfikacyjnych (zarówno biograficznych, jak i biometrycznych); innymi słowy – użytkownik końcowy mógłby przeprowadzać pojedyncze wyszukiwania i otrzymywać wyniki ze wszystkich systemów, do których ma uprawniony dostęp, zamiast oddzielnie przeszukiwać każdy system; jeśli dane istnieją, to system je znajdzie; w przypadku podejrzenia o przestępstwo lub działalność terrorystyczną pierwsze trafienie może być neutralne dla kontrolowanej osoby (tzw. *non hit*), jeśli jednak informacja znajdzie potwierdzenie w drugiej informacji (tzw. *hit*) istniejącej w takich bazach jak SIS, EES, ETIAS, może to skutkować dalszym badaniem i wszczęciem śledztwa;
2) **wspólny serwis kojarzenia danych biometrycznych** – byłby technicznym narzędziem ułatwiającym identyfikację osoby fizycznej, która może być zarejestrowana w różnych bazach danych; przechowywano by w nim wzory danych biometrycznych (odciski palców i wizerunki twarzy) zawarte w centralizowanych systemach informacyjnych UE, tj. SIS, Eurodac, EES, VIS oraz ECRIS-TCN; umożliwiłoby to z jednej strony jednoczesne wyszukiwanie danych biometrycznych przechowywanych w różnych systemach, a z drugiej – porównanie tych danych;
3) **wspólne repozytorium tożsamości** – ułatwiałoby identyfikację osób będących obywatelami państw trzecich znajdujących się na granicy lub w państwach

[38] Na podstawie *Europejskiego programu w zakresie migracji* i następujących po nim komunikatów, w tym komunikatu na temat utrzymania i umocnienia strefy Schengen.

[39] Przez odwołanie się do *Europejskiej agendy bezpieczeństwa* oraz działań Komisji na rzecz rzeczywistej i skutecznej unii bezpieczeństwa.

członkowskich strefy Schengen; umożliwiałoby to organom ścigania dostęp do systemów informacji nieprawnych; w repozytorium przechowywane byłyby dane biograficzne i biometryczne zarejestrowane w systemach VIS, ECRIS-TCN, EES, Eurodac i ETIAS; dane byłyby przechowywane – logicznie oddzielone – w zależności od systemu, z którego pochodziłyby;

4) **moduł wykrywający multiplikacje tożsamości** – byłby narzędziem umożliwiającym łączenie danych identyfikacyjnych w ramach wspólnego repozytorium tożsamości i SIS oraz przechowywanie łączy między rejestrami; gromadzone byłyby tutaj linki dostarczające informacji w przypadku wykrycia jednej lub większej liczby realnych lub możliwych dopasowań; moduł sprawdzałby, czy poszukiwane dane istnieją w więcej niż w jednym systemie, w celu wykrycia wielu tożsamości (np. te same dane biometryczne połączone z różnymi danymi biograficznymi lub te same/podobne dane biograficzne połączone z różnymi danymi biometrycznymi); przedstawiano by wpisy biograficzne dotyczące tożsamości, które mają podobne połączenia w innych systemach.

Dzięki tym czterem elementom interoperacyjności dążono by do tego, aby:

- zapewnienić użytkownikom końcowym (zwłaszcza funkcjonariuszom straży granicznej, funkcjonariuszom organów ścigania, organom sądowym i urzędnikom imigracyjnym) sprawny, szybki, systematyczny i kontrolowany dostęp do odpowiednich systemów informacyjnych;
- ułatwić kontrolę tożsamości obywateli państw trzecich na terytorium państw członkowskich UE;
- wykrywać różne tożsamości powiązane z tym samym zestawem danych;
- usprawnić dostęp organów ścigania do systemów informacyjnych niezwiązanych z organami ścigania.

Dodatkowo wnioski nr 1 i 2 mają na celu wdrożenie dwuetapowego procesu dostępu organów ścigania do wspólnego systemu repozytorium tożsamości w celu zapobiegania, wykrywania i ścigania przestępstw terrorystycznych oraz innych poważnych przestępstw (por. art. 22 obu wniosków). Na pierwszym etapie funkcjonariusz organów ścigania formułowałby zapytanie dotyczące poszukiwanej osoby przy wykorzystaniu danych dotyczących jej tożsamości, danych jej dokumentu podróży lub danych biometrycznych. W ten sposób mógłby sprawdzić, czy dane takiej osoby są przechowywane we wspólnym repozytorium tożsamości. Jeżeli byłyby tam, to funkcjonariusz otrzymałby odpowiedź wskazującą, które systemy informacyjne UE je zawierają. Natomiast nie miałby rzeczywistego dostępu do nich w żadnym z systemów podstawowych.

Na drugim etapie funkcjonariusz organu ścigania mógłby indywidualnie zwrócić się o dostęp do każdego systemu wskazanego jako zawierający dane, aby uzyskać

pełne akta osobowe będące przedmiotem zapytania zgodnie z obowiązującymi przepisami i procedurami ustanowionymi dla każdego systemu. Dostęp w ramach tego etapu wymagałby uprzedniej autoryzacji, którą przyznawałby właściwy organ, oraz – w dalszym ciągu – posiadania ID użytkownika i zalogowania się do systemu.

Ponadto wnioski nr 1 i 2 obejmują dodatkowe elementy wspierające interoperacyjność. Dotyczy to chociażby ustanowienia centralnego repozytorium sprawozdawczo-statystycznego. W założeniu ma ono wspierać realizację celów systemów informacyjnych oraz generować międzysystemowe dane statystyczne i sprawozdania analityczne służące strategiom politycznym, celom operacyjnym i związanym z jakością danych (por. art. 39). Jest w nich także mowa o ustanowieniu uniwersalnego formatu wiadomości – UMF, który wprowadziłby wspólny, jednolity język techniczny służący opisywaniu i łączeniu elementów danych, zwłaszcza elementów związanych z osobami oraz dokumentami podróży. Korzystanie z tego standardu ma gwarantować łatwiejszą integrację i interoperacyjność z innymi systemami (por. art. 38).

Wnioski nr 1 i 2 wprowadzają również koncepcję zautomatyzowanych mechanizmów kontroli jakości danych (art. 37). Mechanizmy takie mają obejmować wdrażanie automatycznych reguł walidacji przy wprowadzaniu danych oraz ustanawiać wspólne wskaźniki jakości danych i minimalnych standardów jakości. Mimo że w art. 37 wniosków nr 1 i 2 przewidziano, iż zostaną one opracowane, i wyszczególniono powiązane role i obowiązki, nierozwiązany pozostał jeszcze jednak problem rozwoju tych zautomatyzowanych mechanizmów.

3. Ocena skuteczności propozycji w sprawie interoperacyjności

W dzisiejszych czasach, kiedy mamy do czynienia z ogromną ilością danych (ang. *big data*), kwestia tego, czy informacje pochodzące z różnych źródeł zostaną połączone lub też nie w celu tworzenia indywidualnych profili, staje się już tylko kwestią ograniczeń prawnych, a nie technologicznych, ponieważ te ostatnie stopniowo tracą na znaczeniu[40]. Dzięki coraz doskonalszym rozwiązaniom technologicznym działania zmierzające do zapewnienia interoperacyjności systemów informacyjnych stają się jeszcze bardziej oczywiste i pożądane.

Zakładana interoperacyjność systemów informacyjnych ma przede wszystkim umożliwić właściwym organom szybki, płynny, systematyczny i kontrolowany dostęp

[40] Zob. m.in.: D. Broeders, *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, „International Sociology" 2007, vol. 22, issue 1, s. 77; P. de Hert, S. Gutwirth, op.cit., s. 25.

do określonych informacji. Proponowane rozwiązania pozwalają na wykrywanie wielu tożsamości, co niewątpliwie ułatwia kontrolę tożsamości obywateli państw trzecich oraz usprawnia dostęp organów ścigania do systemów informacyjnych. W kontekście azylu, granic i bezpieczeństwa właściwy organ, korzystając z interoperacyjnego systemu, będzie mógł uzyskać informacje na temat wcześniejszych zachowań osób podróżujących, wniosków wizowych, istniejących zakazów ponownego wjazdu czy wniosków azylowych w jednym wyszukiwaniu[41].

Należy także pamiętać, że wciąż utrzymujące się zagrożenie terrorystyczne, a także trwający w Unii Europejskiej kryzys migracyjny stanowią poważne wyzwania dla strefy Schengen (jako bezpiecznej strefy bez stałej kontroli na granicach wewnętrznych). Sprawne funkcjonowanie instrumentów wymiany informacji pomiędzy uprawnionymi organami i maksymalnie efektywne wykorzystanie zawartych w nich danych jest zatem niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa wewnętrznego w państwach członkowskich strefy Schengen.

Występujące w obecnej architekturze wymiany informacji luki, m.in. zbyt skomplikowany proces dostępu organów ścigania do systemów, brak pełnej dostępności informacji na granicy o wszystkich kategoriach podróżnych oraz pojawiający się problem słabej jakości danych, którymi zasilane są systemy, sprawiają, że unijne systemy informacyjne nie są obecnie w pełni interoperacyjne. Dalsze usprawnianie funkcjonowania wielkoskalowych systemów informacyjnych UE, które wspierają proces kontroli na granicach zewnętrznych UE oraz są wykorzystywane przez organy ścigania (zgodnie z wymogami ochrony danych osobowych), wydaje się zatem uzasadnione.

Zgodnie z wnioskami nr 1 i 2 interoperacyjność systemów informacyjnych ma usprawnić procesy decyzyjne oraz zwiększyć dokładność danych alfanumerycznych, które są systematycznie porównywane z danymi biometrycznymi. Rozszerzone wykorzystywanie danych biometrycznych w celu identyfikacji obywateli państw trzecich spowoduje, że taka identyfikacja będzie bardziej wiarygodna oraz zostaną uzyskane dokładniejsze wyniki. Nie tylko byłoby to niezmiernie korzystne dla organów przetwarzających dane osobowe obywateli państw trzecich, lecz także przyspieszyłoby średni czas rozpatrywania wniosków wizowych, skróciłoby czas oczekiwania na przejściach granicznych oraz pozwoliłoby oddzielić osoby podróżujące w dobrej wierze od innych osób.

Przeprowadzana weryfikacja systemów informacyjnych UE ułatwi wykrywanie fałszywych tożsamości i podrobionych dokumentów. Może też przyczynić się do: zapobieżenia ponownemu wjazdowi przestępców i osób, którym odmówiono wniosku o azyl, efektywniejszego wykrywania zaginionych dzieci, potwierdzenia

[41] T. Quintel, op.cit., s. 12.

prawdziwości wniosków o azyl i wykrywania ofiar handlu ludźmi[42]. Jeśli jednak te systemy informacyjne będą zawierać niedokładne dane, co obecnie ma miejsce[43], to wykorzystywanie danych może doprowadzić do pewnych nieprawidłowości, błędnych dopasowań i znacznej liczby fałszywych trafień.

Wnioski nr 1 i 2 tworzą nową, scentralizowaną bazę danych, która będzie zawierać informacje o milionach obywateli państw trzecich, w tym ich dane biometryczne. Ze względu na skalę i charakter danych, które mają być przechowywane w tej bazie danych, wszelkie naruszenia bezpieczeństwa danych mogłyby poważnie zaszkodzić bardzo dużej liczbie osób fizycznych. Jeżeli takie informacje kiedykolwiek znalazłyby się w posiadaniu niewłaściwych osób, baza danych mogłaby stać się niebezpiecznym narzędziem wykorzystywanym z naruszeniem praw podstawowych jednostki. Dlatego, jak słusznie zauważa w swojej opinii EIOD, konieczne jest stworzenie silnych zabezpieczeń prawnych, technicznych i organizacyjnych[44]. Szczególną przezorność należy więc zachować w kontekście zarówno celów tworzenia bazy danych, jak i warunków oraz sposobów jej wykorzystania.

Opracowanie wniosków nr 1 i 2 może sprawiać wrażenie osiągnięcia interoperacyjności jako finalnego rezultatu już w pełni funkcjonujących systemów informacyjnych (lub przynajmniej systemów, których akty założycielskie są już „stabilne" i znajdują się w końcowej fazie procesu legislacyjnego). Tak jednak nie jest. W rzeczywistości bowiem obecnie nie funkcjonują jeszcze trzy z sześciu systemów informacyjnych UE, które mają zostać połączone zgodnie z tymi wnioskami (system ETIAS, ECRIS-TCN i EES), dwa kolejne są obecnie poddawane przeglądowi (system SIS i Eurodac), a jeden ma zostać jemu poddany jeszcze w tym roku (system VIS).

Ocena pod względem ochrony danych osobowych bardzo złożonego systemu z tak dużą liczbą „ruchomych części" jest prawie niemożliwa. Ważne jest więc zapewnienie spójności między już negocjowanymi (lub przyszłymi) tekstami prawnymi a wnioskami nr 1 i 2 w celu zapewnienia jednolitego otoczenia prawnego, organizacyjnego i technicznego dla wszystkich działań związanych z przetwarzaniem danych osobowych w Unii.

Początkowo interoperacyjność była planowana jako narzędzie ułatwiające jedynie korzystanie z systemów informacyjnych UE. Natomiast wnioski nr 1 i 2 wprowadzają nowe możliwości dostępu do danych przechowywanych w różnych systemach i ich wykorzystywania w celu zwalczania oszustw dotyczących tożsamości, a także

---

[42] Ibidem, s. 14–15.

[43] Euobserver, *Inaccurate data in Schengen system 'threatens rights'*, 08.01.2018, https://euobserver.com/tickers/140468 [dostęp 01.09.2018].

[44] Zob. European Data Protection Supervisor, Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16.04.2018, s. 3, https://edps.europa.eu/sites/edp/files/publication/2018–04-16_interoperability_opinion_en.pdf [dostęp 01.09.2018].

ułatwiania kontroli tożsamości i usprawniania dostępu organów ścigania do nieprawnych systemów informacyjnych.

Jeżeli chodzi o wykorzystanie danych przechowywanych w różnych systemach z myślą o ułatwieniu kontroli tożsamości na terytoriach państw członkowskich, to powody takiego wykorzystania, tj. zwalczanie nielegalnej migracji i przyczynianie się do wysokiego poziomu bezpieczeństwa, zostały sformułowane zbyt szeroko i powinny zostać ograniczone i precyzyjnie dookreślone we wnioskach nr 1 i 2, tak aby były zgodne z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE). I tak dostęp do wspólnego repozytorium tożsamości w celu ustalenia tożsamości obywatela państwa trzeciego, aby zapewnić wysoki poziom bezpieczeństwa, powinien być dozwolony jedynie w przypadku, gdy istnieje dostęp do podobnych krajowych baz danych w tym samym celu (np. rejestr obywateli/mieszkańców) i na tych samych warunkach. Wartościowe byłoby wyraźne doprecyzowanie tego w tych wnioskach. Wydaje się bowiem, że w przeciwnym razie wnioski nr 1 i 2 ustanowią domniemanie, iż obywatele państw trzecich z definicji stanowią zagrożenie dla bezpieczeństwa.

Istotne jest dokonanie oceny proponowanych rozwiązań zawartych we wnioskach nr 1 i 2 również z perspektywy interesów jednostki. Szczególny problem w tym kontekście wiąże się z faktem, że dotyczą one interoperacyjności unijnych systemów informacyjnych, nie tylko mających różne cele, lecz także obejmujących różne kategorie osób, których te dane dotyczą. Systemy te zawierają bowiem dane osób fizycznych, gdy wiążą się one z zachowaniem przestępczym lub nielegalnym przekraczaniem granicy, ale również dane osób podróżujących w dobrej wierze (umieszczane w systemie Eurodac i VIS). Należy zaznaczyć, że interoperacyjność nie doprowadzi do pomieszania tych kategorii.

Wydaje się także, że wnioski nr 1 i 2 zwiększają ryzyko dyskryminacji obywateli państw trzecich oraz osób określonego pochodzenia rasowego lub etnicznego. Artykuł 5 (*Zakaz dyskryminacji*) ma zastosowanie wyłącznie do przetwarzania danych osobowych, nie usuwa jednak dyskryminującego charakteru tych wniosków ani ewentualnego dyskryminującego wpływu na obywateli państw trzecich konkretnych kontroli na podstawie mechanizmu interoperacyjności.

Także w odniesieniu do jednego z celów wniosków nr 1 i 2, tj. ułatwienia i usprawnienia dostępu organów ścigania do unijnych baz danych, pojawiają się wątpliwości dotyczące konieczności i proporcjonalności takiego różnego traktowania obywateli Unii i obywateli państw trzecich (w tym członków rodzin obywateli Unii, osób ubiegających się o azyl czy o wizę Schengen). W uzasadnieniu do wniosków nr 1 i 2 wskazuje się bowiem różne traktowanie obywateli Unii i obywateli państw trzecich, mające pomóc w zachowaniu bezpieczeństwa w Unii. Stanowi się tam, że „choć

wnioski te nie dotyczą bezpośrednio obywateli UE, to oczekuje się, że zwiększą one zaufanie społeczeństwa dzięki zapewnieniu, że ich konstrukcja i stosowanie poprawia bezpieczeństwo obywateli Unii"[45]. Uzasadnienie takie oznacza w zasadzie, że obywatele państw trzecich – nawet jeśli nie mają związku z żadnym nielegalnym zachowaniem – powinni podlegać dodatkowym kontrolom bezpieczeństwa, aby obywatele Unii mogli czuć się bezpieczniej. Ponadto jeden ze szczegółowych celów wniosków nr 1 i 2 – tj. ułatwienie kontrolowania tożsamości obywateli państw trzecich na terytorium UE przez organy policji, aby sprawdzić, czy informacje na temat tej osoby są przechowywane w jednej bazie danych, czy w kilku bazach danych UE – może zwiększyć możliwość zatrzymywania obywateli państw trzecich (lub osób uważanych za obywateli państw trzecich) do kontroli tożsamości.

W uzasadnieniu do wniosków nr 1 i 2 pojawia się także jedynie bardzo ogólne zapewnienie, że standardy dotyczące ochrony danych osobowych zostały spełnione[46]. Nie podaje się jednak wyraźnego uzasadnienia, w jaki sposób wnioski spełniają te standardy, określone zarówno w art. 8 KPP (*Ochrona danych osobowych*), jak i w innych unijnych instrumentach prawnych przyjętych na podstawie art. 16 TFUE. Wnioski nr 1 i 2 powinny być szczegółowo wsparte przez ocenę proporcjonalności ingerencji w prawo do ochrony danych osobowych, zgodnie z wymogami określonymi przez art. 8 i art. 52 ust. 1 KPP, jak i zasadami wypracowanymi przez orzecznictwo TSUE[47]. Nie jest też jasne, w jaki sposób wnioski nr 1 i 2 pozostają spójne z ogólnym rozporządzeniem o ochronie danych[48] i dyrektywą 2016/680, regulującą ochronę danych osobowych w obszarze prawa karnego i współpracy organów, których zadaniem jest zwalczanie przestępczości[49]. Z uwagi na to, że mamy do czynienia z wieloma systemami informacyjnymi, które zawierają różne dane, i że różne są cele, dla których te dane są przetwarzane, konieczne wydaje się wyraźne określenie we wnioskach, kiedy miałoby zastosowanie ogólne rozporządzenie o ochronie danych, a kiedy dyrektywa 2016/680.

---

45 Wnioski nr 1 i 2, s. 20.

46 Ibidem, s. 22.

47 Zob. m.in. wyrok Trybunału z 8 kwietnia 2014 r. w sprawach połączonych C-293/12 i C-594/12 *Digital Rights Ireland i Seitlinger i in.*, ECLI:EU:C:2014:238.

48 Zob. 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), Dz. Urz. UE 2016 L 119/1.

49 Zob.: dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz. Urz. UE 2016 L 119/89.

Zgodnie z uzasadnieniem do wniosków nr 1 i 2 „dostęp do danych jest zarezerwowany wyłącznie dla odpowiednio uprawnionego personelu organów państw członkowskich w konkretnych celach dla każdego systemu informacyjnego i jest ograniczony do zakresu, w jakim te dane są konieczne do wykonywania zadań zgodnie z tymi celami”[50]. Tym samym wnioski nie zmieniają szczególnych celów, dla których utworzono unijne bazy danych. Jednak zgodnie z ich postanowieniami każdy wyznaczony organ państw członkowskich będzie mógł za pośrednictwem europejskiego portalu wyszukiwania dowiedzieć się, czy informacje dotyczące obywatela państwa trzeciego są przechowywane w jednej z takich baz. Innymi słowy, dostęp takich organów do europejskiego portalu wyszukiwania nie ogranicza się do ich szczególnych kompetencji lub zadań, natomiast te szczególne kompetencje lub zadania ograniczają obecnie dostęp tych organów do konkretnych unijnych baz danych.

Informacje zebrane za pośrednictwem europejskiego portalu wyszukiwania pozwolą ustalić, czy ktoś jest uwzględniony np. w systemie Eurodac, czy w SIS. Oznacza to tym samym rozszerzenie celu tych baz danych – nawet jeżeli dostęp do danych osobowych w tej bazie danych nie jest możliwy ze względu na brak zezwolenia, stosowny organ i tak uzyska wiedzę o istnieniu takich danych. Co więcej, sama wiedza o tym, że dane takiej osoby znajdują się w konkretnym systemie informacyjnym, daje organowi informacje o działaniach tej osoby. Może to stanowić ingerencję w prawo do ochrony danych osobowych określonych w art. 7 (*Poszanowanie życia prywatnego i rodzinnego*) i art. 8 KPP[51].

We wnioskach nr 1 i 2 nie określono wyraźnie okresu przechowywania danych zgromadzonych przez uprawnione organy. Obecnie prawo unijne przewiduje różne terminy przechowywania danych osobowych zawartych w różnych bazach danych UE (Eurodac – 10 lat i 2 lata, VIS – 5 lat, SIS – 3 lata z możliwością przedłużenia). Wnioski nr 1 i 2 nie zmieniają tych terminów, jednak pozostaje niejasne, które okresy przechowywania danych zostaną uwzględnione, gdy informacje będą przechowywane we wspólnym repozytorium tożsamości. Zgodnie bowiem z art. 23 wniosków: „Akta osobowe są przechowywane we wspólnym repozytorium tożsamości tak długo, jak długo są one przechowywane w co najmniej jednym systemie informacyjnym, którego dane są zawarte w repozytorium. Stworzenie powiązania nie wpływa na okres zatrzymywania żadnej z pozycji wchodzącej w skład powiązanych danych”.

---

[50] Wnioski nr 1 i 2, s. 22.

[51] Meijers Committee, CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM(2017) 794, 19.02.2018, s. 5, https://www.commissie-meijers.nl/sites/all/files/cm1802_comments_on_com_2017_794.pdf [dostęp 01.09.2018].

Oznacza to, że okres zatrzymywania danych jest powiązany z czasem, który pozwala na najdłuższy okres ich przechowywania. Jeśli więc np. zgodnie z rozporządzeniem w sprawie VIS informacje dotyczące wnioskodawcy ubiegającego się o wizę powinny zostać usunięte z VIS, a jego odciski palców są również przechowywane w systemie Eurodac, to dane takiej osoby mogą pozostać we wspólnym repozytorium tożsamości przez ponad 5 lat, łącznie z informacją, że plik został zapisany w systemie VIS dla tej osoby. Zmienia to wskazane okresy zatrzymywania danych, co nie jest zgodne zarówno z przepisami dotyczącymi zatrzymywania danych przewidzianymi przez specjalne instrumenty prawne ustanawiające odpowiednie bazy danych, jak i z zasadą zatrzymywania danych, określoną w art. 5 ust. 1 lit. e) ogólnego rozporządzenia o ochronie danych oraz art. 4 ust. 1 lit. e) dyrektywy 2016/680.

Warto się także zastanowić, w jaki sposób można zagwarantować skuteczną realizację prawa dostępu do danych oraz żądanie ich sprostowania i usunięcia, zgodnie z art. 47 wniosków nr 1 i 2. Obecne praktyki w tym zakresie w odniesieniu do systemu SIS i praw osób fizycznych dotyczących tego systemu pokazują, że w państwach członkowskich UE takim osobom niezwykle trudno jest egzekwować to prawo[52]. Problem ten prawdopodobnie stanie się bardziej kłopotliwy, jeśli przez wprowadzenie interoperacyjności zostanie zaangażowanych jeszcze więcej systemów informacyjnych oraz upoważnionych organów państw członkowskich UE.

Podsumowanie

Interoperacyjność oznacza zdolność różnych systemów informacyjnych do komunikowania się, wymiany danych i wykorzystywania wymienianych informacji, z poszanowaniem uprawnień dostępu do systemów. Powinna ona być wdrażana w sposób przemyślany i w pełnej zgodności z prawami podstawowymi (w tym prawem do prywatności i ochrony danych osobowych). Wówczas może być użytecznym narzędziem służącym zaspokajaniu uzasadnionych potrzeb właściwych organów korzystających z wielkoskalowych systemów informacyjnych, a także przyczynić się do rozwoju skutecznej i wydajnej wymiany informacji. Interoperacyjność jest nie tylko kwestią techniczną, ale nawet bardziej polityczną, która może mieć poważne konsekwencje prawne i społeczne.

---

[52] Zob.: E. Brouwer, *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden–Boston 2008; European Data Protection Supervisor, Reflection paper on the interoperability of information systems in the Area of Freedom, Security and Justice, 17.11.2017, https://edps.europa.eu/sites/edp/files/publication/17–11-16_opinion_interoperability_en.pdf [dostęp 01.09.2018].

Obecnie można zauważyć wyraźną tendencję do osiągania kompatybilności celów politycznych UE i przepisów dotyczących odprawy granicznej, azylu i imigracji, współpracy policyjnej oraz współpracy sądowej w sprawach karnych, jak również przyznawania organom ścigania rutynowego dostępu do systemów informacyjnych niezwiązanych z bazami danych takich organów. Stąd decyzja o uczynieniu wielkoskalowych systemów informacyjnych UE interoperacyjnymi nie tylko w sposób trwały i głęboki wpłynie na ich strukturę i sposób funkcjonowania, ale zmieni także sposób, w jaki do tej pory były interpretowane zasady prawne w tej dziedzinie.

Z założenia interoperacyjność ma pozwolić na sprawniejsze wykrywanie osób stanowiących zagrożenie dla bezpieczeństwa nie tylko wtedy, gdy przekraczają granice zewnętrzne UE, lecz także gdy przemieszczają się wewnątrz strefy Schengen. Stworzenie czterech nowych narzędzi interoperacyjności (europejskiego portalu wyszukiwania, wspólnego serwisu kojarzenia danych biometrycznych, wspólnego repozytorium tożsamosci, modułu wykrywającego multiplikację tożsamości) ma ułatwić detekcję osób posługujących się nielegalnie wieloma tożsamościami oraz pozwolić na podejmowanie przez uprawnione organy decyzji mających pełniejsze umocowanie w podstawach faktycznych.

Brak interoperacyjności systemów informacyjnych UE niewątpliwie utrudnia pracę upoważnionych użytkowników (m.in. pracowników straży granicznej, funkcjonariuszy organów ścigania, urzędników imigracyjnych, urzędników wizowych czy organów sądowych). Rozdrobniona architektura danych służących do zarządzania bezpieczeństwem, granicami i migracją może być także przyczyną istnienia słabych punktów, mającego konsekwencje dla bezpieczeństwa wewnętrznego UE. Kontrole osób na granicach zewnętrznych UE nie są wystarczająco skuteczne, aby właściwie zarządzać przepływami migracyjnymi i zwiększać bezpieczeństwo wewnętrzne. Dowodem tego są nieustanne przypadki niedozwolonego przekraczania granic UE i coraz większe zagrożenie bezpieczeństwa wewnętrznego, czego przejawem była cała seria ataków terrorystycznych.

Za główne skutki społeczne wniosków nr 1 i 2 można uznać wzmocnienie zarządzania granicami i zwiększenie bezpieczeństwa wewnętrznego. Bardziej spójne zarządzanie danymi tożsamościowymi oraz usprawnienie dostępu do systemów kontroli granic i imigracji będzie miało korzystny wpływ na współpracę policyjną i ściganie przestępstw.

W uzasadnieniu do wniosków nr 1 i 2 wskazuje się, że interoperacyjność będzie oznaczać bezpośrednie oszczędności o wartości szacowanej na 77,5 mln EUR rocznie (prawie w całości po stronie administracji państw członkowskich). Oszczędności te mają wynikać głównie ze zmniejszenia kosztów szkoleń okresowych oraz

z ograniczenia nakładu pracy koniecznej do wyjaśniania przypadków multiplikacji tożsamości i wykrywania oszustw dotyczących tożsamości.

Koszty projektowania i eksploatacji infrastruktury przewidywanej we wnioskach zostaną pokryte z budżetu UE i przez organy państw członkowskich korzystające z systemów. Jednorazowy łączny koszt szacuje się na 169,8 mln EUR. Przypuszczalnie zostanie on podzielony niemal po równo między państwa członkowskie UE (50,3%) i samą UE (49,7%). Natomiast udział w rocznych kosztach bieżących w wysokości 28,5 mln EUR będą ponosiły w ponad 60% państwa członkowskie UE.

INTEROPERABILITY OF EU INFORMATION SYSTEMS FOR SECURITY, BORDER PROTECTION AND MIGRATION MANAGEMENT

Abstract

In recent years, the European Union (EU) has experienced an increase in irregular border crossings. The checks on persons at the EU's external borders should therefore be more effective to improve, i.a., efficient management of migration flows. It has become a particularly urgent need to join up and strengthen in a comprehensive manner the EU's information tools for border management and preventing and combating illegal immigration. The article concerns the issue of ensuring interoperability between EU centralized information systems in the area of freedom, security and justice. It turns out that the existing systems do not cooperate with each other. For this purpose, interoperability components need to be established: European search portal, shared biometric matching service, common identity repository and multiple-identity detector.

Keywords: European Union, information systems, protection of external borders, interoperability, area of freedom, security and justice

Bibliografia

1. Broeders D., *The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants*, „International Sociology" 2007, vol. 22, issue 1, s. 71–92.
2. Brouwer E., *Digital Borders and Real Rights. Effective remedies for third-country nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden–Boston 2008.

3. Council of the European Union, Additional measures to combat terrorism – proposals by the German delegation, 13176/01, Brussels, 24.10.2001.
4. Council of the European Union, Declaration condemning the terrorists attacks on London, 11116/05, Brussels, 13.07.2005 (Presse 187).
5. Council of the European Union, Declaration on combating terrorism, 7906/04, Brussels, 29.03.2004.
6. Council of the European Union, Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area, 9368/1/16, Brussels, 06.06.2016.
7. De Hert P., Gurtwirth S., *Interoperability of Police Databases within the EU: An Accountable Political Choice?*, „International Review of Law Computers and Technology" 2006, vol. 20, issue 1–2, s. 21–35.
8. Decyzja Komisji z dnia 17 czerwca 2016 r. ustanawiająca grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności (2016/C 257/03), Dz. Urz. UE 2016 C 257/03.
9. Decyzja Rady 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz. Urz. UE 2004 L 213/5.
10. Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE 2007 L 205/63.
11. Decyzja Rady 2009/316/WSiSW z dnia 6 kwietnia 2009 r. w sprawie ustanowienia europejskiego systemu przekazywania informacji z rejestrów karnych (ECRIS), zgodnie z art. 11 decyzji ramowej 2009/315/WSiSW, Dz. Urz. UE 2009 L 93/33.
12. Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, Dz. Urz. UE 2009 L 93/23.
13. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz. Urz. UE 2016 L 119/89.
14. Euobserver, *Inaccurate data in Schengen system 'threatens rights'*, 08.01.2018, https://euobserver.com/tickers/140468 [dostęp 01.09.2018].
15. European Commission, Development of the Schengen Information System II, COM(2001) 720 final, Brussels, 18.12.2001.
16. European Council, European Council meeting (17 and 18 December 2015) – Conclusions, EUCO 28/15, Brussels, 18.12.2015.

17. European Council, European Council meeting (15 December 2016) – Conclusions, EUCO 34/16, Brussels, 15.12.2016.
18. European Council, European Council meeting (22 and 23 June 2017) – Conclusions, EUCO 8/17, Brussels, 23.06.2017.
19. European Data Protection Supervisor, Comments on the Communication of the Commission on interoperability of European databases, Brussels, 10.03.2006, https://edps.europa.eu/sites/edp/files/publication/06–03-10_interoperability_en.pdf [dostęp 01.09.2018].
20. European Data Protection Supervisor, Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, 16.04.2018, https://edps.europa.eu/sites/edp/files/publication/2018–04-16_interoperability_opinion_en.pdf [dostęp 01.09.2018].
21. European Data Protection Supervisor, Reflection paper on the interoperability of information systems in the Area of Freedom, Security and Justice, 17.11.2017, https://edps.europa.eu/sites/edp/files/publication/17–11-16_opinion_interoperability_en.pdf [dostęp 01.09.2018].
22. European Data Protection Supervisor statement on the concept of interoperability in the field of migration, asylum and security, https://edps.europa.eu/sites/edp/files/publication/17–05-08_statement_on_interoperability_en.pdf [dostęp 01.09.2018].
23. European Parliament, Interoperability of Justice and Home Affairs Information Systems. Study, April 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU (2018) 604947_EN.pdf [dostęp 01.09.2018].
24. *High-level expert group on information systems and interoperability. Final report*, 2017, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1 [dostęp 01.09.2018].
25. Komisja Europejska, Komunikat: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, COM(2016) 205, Bruksela, 06.04.2016.
26. Komisja Europejska, Komunikat w sprawie zwiększenia skuteczności, interoperacyjności i efektu synergii wynikającego ze współdziałania europejskich baz danych w dziedzinie sprawiedliwości i spraw wewnętrznych, COM(2005) 597 końcowy, Bruksela, 24.11.2005.
27. Komisja Europejska, Program prac Komisji na 2018 r. Plan działania na rzecz bardziej zjednoczonej, silniejszej i bardziej demokratycznej Unii, COM(2017) 650 final, Bruksela, 24.10.2017.

28. Komisja Europejska, Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające 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, Strasburg, 12.12.2017.
29. Komisja Europejska, Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja), COM(2017) 794, Strasburg, 12.12.2017.
30. Komisja Europejska, Zmieniony wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności między systemami informacyjnymi UE (w obszarze granic i polityki wizowej) oraz zmieniające decyzję Rady 2004/512/WE, rozporządzenie (WE) nr 767/2008, decyzję Rady 2008/633/WSiSW, rozporządzenie (UE) 2016/399, rozporządzenie (UE) 2017/2226, rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie ETIAS], rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie SIS w odniesieniu do odpraw granicznych] oraz rozporządzenie (UE) 2018/XX, COM(2018) 478, Bruksela, 13.06.2018.
31. Komisja Europejska, Zmieniony wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ustanowienia ram interoperacyjności pomiędzy systemami informacyjnymi UE (współpraca policyjna i sądowa, azyl i migracja) oraz zmieniające [rozporządzenie (UE) 2018/XX [rozporządzenie Eurodac], rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie SIS w odniesieniu do ścigania przestępstw], rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie ECRIS-TCN] oraz rozporządzenie (UE) 2018/XX [rozporządzenie w sprawie eu-LISA], COM(2018) 480, Bruksela, 13.06.2018.
32. Meijers Committee, CM1802 Comments on the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) 12 December 2017, COM(2017) 794, 19.02.2018, https://www.commissie-meijers.nl/sites/all/files/cm1802_comments_on_com_2017_794.pdf [dostęp 01.09.2018].
33. Quintel T., *Connecting personal data of Third Country Nationals. Interoperability of EU databases in the light of the CJEU's case law on data retention*, „Law Working Paper Series" 2018, no. 2, s. 1–18, https://www.researchgate.net/publication/323924372_Connecting_Personal_Data_of_Third_Country_Nationals_Interoperability_of_EU_Databases_in_the_Light_of_the_CJEU's_Case_Law_on_Data_Retention [dostęp 01.09.2018].
34. Rada, Program Haski: wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, Dz. Urz. UE 2005 C 53/01.

35. Rada Unii Europejskiej, Wspólne oświadczenie unijnych ministrów sprawiedliwości i spraw wewnętrznych oraz przedstawicieli instytucji UE w sprawie zamachów terrorystycznych, do których doszło w Brukseli 22 marca 2016 r., 7371/16, Bruksela, 24.03.2016.
36. 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), Dz. Urz. UE 2016 L 119/1.
37. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226, Dz. Urz. UE 2018 L 236/1.
38. Rozporządzenie (WE) nr 1986/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie dostępu służb odpowiedzialnych w państwach członkowskich za wydawanie świadectw rejestracji pojazdów do Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE 2006 L 381/1.
39. Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE 2006 L 381/4.